**[MS-NRPC]:**

**Netlogon Remote Protocol**

Intellectual Property Rights Notice for Open Specifications Documentation

* **Technical Documentation.** Microsoft publishes Open Specifications documentation (“this documentation”) for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
* **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
* **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
* **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft [Open Specifications Promise](http://go.microsoft.com/fwlink/?LinkId=214445) or the [Microsoft Community Promise](http://go.microsoft.com/fwlink/?LinkId=214448). If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting [iplg@microsoft.com](mailto:iplg@microsoft.com).
* **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the [Patent Map](https://msdn.microsoft.com/en-us/openspecifications/dn750984).
* **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit [www.microsoft.com/trademarks](http://www.microsoft.com/trademarks).
* **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

**Reservation of Rights**. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

**Tools**. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

**Support.** For questions and support, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

**Revision Summary**

| Date | Revision History | Revision Class | Comments |
| --- | --- | --- | --- |
| 12/18/2006 | 0.01 | New | Version 0.01 release |
| 3/2/2007 | 1.0 | Major | Version 1.0 release |
| 4/3/2007 | 1.1 | Minor | Version 1.1 release |
| 5/11/2007 | 1.2 | Minor | Version 1.2 release |
| 6/1/2007 | 1.2.1 | Editorial | Changed language and formatting in the technical content. |
| 7/3/2007 | 2.0 | Major | Technical changes were made to existing sections. |
| 7/20/2007 | 2.1 | Minor | Made technical and editorial changes based on feedback. |
| 8/10/2007 | 2.2 | Minor | Updated content based on feedback. |
| 9/28/2007 | 2.3 | Minor | Made technical and editorial changes based on feedback. |
| 10/23/2007 | 2.4 | Minor | Made technical and editorial changes based on feedback. |
| 11/30/2007 | 2.5 | Minor | Made technical changes based on feedback. |
| 1/25/2008 | 2.6 | Minor | Clarified the meaning of the technical content. |
| 3/14/2008 | 2.7 | Minor | Clarified the meaning of the technical content. |
| 5/16/2008 | 3.0 | Major | Updated and revised the technical content. |
| 6/20/2008 | 4.0 | Major | Updated and revised the technical content. |
| 7/25/2008 | 5.0 | Major | Updated and revised the technical content. |
| 8/29/2008 | 6.0 | Major | Updated and revised the technical content. |
| 10/24/2008 | 6.1 | Minor | Clarified the meaning of the technical content. |
| 12/5/2008 | 7.0 | Major | Updated and revised the technical content. |
| 1/16/2009 | 7.1 | Minor | Clarified the meaning of the technical content. |
| 2/27/2009 | 8.0 | Major | Updated and revised the technical content. |
| 4/10/2009 | 9.0 | Major | Updated and revised the technical content. |
| 5/22/2009 | 9.1 | Minor | Clarified the meaning of the technical content. |
| 7/2/2009 | 10.0 | Major | Updated and revised the technical content. |
| 8/14/2009 | 11.0 | Major | Updated and revised the technical content. |
| 9/25/2009 | 12.0 | Major | Updated and revised the technical content. |
| 11/6/2009 | 13.0 | Major | Updated and revised the technical content. |
| 12/18/2009 | 14.0 | Major | Updated and revised the technical content. |
| 1/29/2010 | 15.0 | Major | Updated and revised the technical content. |
| 3/12/2010 | 16.0 | Major | Updated and revised the technical content. |
| 4/23/2010 | 17.0 | Major | Updated and revised the technical content. |
| 6/4/2010 | 18.0 | Major | Updated and revised the technical content. |
| 7/16/2010 | 18.1 | Minor | Clarified the meaning of the technical content. |
| 8/27/2010 | 19.0 | Major | Updated and revised the technical content. |
| 10/8/2010 | 20.0 | Major | Updated and revised the technical content. |
| 11/19/2010 | 21.0 | Major | Updated and revised the technical content. |
| 1/7/2011 | 21.1 | Minor | Clarified the meaning of the technical content. |
| 2/11/2011 | 21.2 | Minor | Clarified the meaning of the technical content. |
| 3/25/2011 | 21.3 | Minor | Clarified the meaning of the technical content. |
| 5/6/2011 | 22.0 | Major | Updated and revised the technical content. |
| 6/17/2011 | 23.0 | Major | Updated and revised the technical content. |
| 9/23/2011 | 23.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 12/16/2011 | 24.0 | Major | Updated and revised the technical content. |
| 3/30/2012 | 25.0 | Major | Updated and revised the technical content. |
| 7/12/2012 | 26.0 | Major | Updated and revised the technical content. |
| 10/25/2012 | 27.0 | Major | Updated and revised the technical content. |
| 1/31/2013 | 28.0 | Major | Updated and revised the technical content. |
| 8/8/2013 | 29.0 | Major | Updated and revised the technical content. |
| 11/14/2013 | 30.0 | Major | Updated and revised the technical content. |
| 2/13/2014 | 30.1 | Minor | Clarified the meaning of the technical content. |
| 5/15/2014 | 31.0 | Major | Updated and revised the technical content. |
| 6/30/2015 | 32.0 | Major | Significantly changed the technical content. |
| 10/16/2015 | 32.0 | None | No changes to the meaning, language, or formatting of the technical content. |
| 7/14/2016 | 33.0 | Major | Significantly changed the technical content. |
| 6/1/2017 | 33.1 | Minor | Clarified the meaning of the technical content. |
| 9/15/2017 | 34.0 | Major | Significantly changed the technical content. |

Table of Contents

[1 Introduction 10](#_Toc492419921)

[1.1 Glossary 10](#_Toc492419922)

[1.2 References 17](#_Toc492419923)

[1.2.1 Normative References 18](#_Toc492419924)

[1.2.2 Informative References 19](#_Toc492419925)

[1.3 Overview 20](#_Toc492419926)

[1.3.1 Pass-Through Authentication 20](#_Toc492419927)

[1.3.2 Pass-Through Authentication and Domain Trusts 21](#_Toc492419928)

[1.3.3 Account Database Replication 22](#_Toc492419929)

[1.3.4 Secure Channel Maintenance 23](#_Toc492419930)

[1.3.5 Domain Trust Services 23](#_Toc492419931)

[1.3.6 Message Protection Services 23](#_Toc492419932)

[1.3.7 Administrative Services 23](#_Toc492419933)

[1.3.7.1 Netlogon Operational Flow on Domain Members 23](#_Toc492419934)

[1.3.7.2 Netlogon Operational Flow on Domain Controllers 24](#_Toc492419935)

[1.3.8 Netlogon Structures and Methods 24](#_Toc492419936)

[1.3.8.1 History of Netlogon 24](#_Toc492419937)

[1.3.8.1.1 New Methods Derived from Existing Methods 25](#_Toc492419938)

[1.3.8.1.2 Using Dummy Fields in Structures 25](#_Toc492419939)

[1.3.8.1.3 Fields and Structures Used by Netlogon Pass-through Methods 25](#_Toc492419940)

[1.3.8.1.4 Using Negotiated Flags 26](#_Toc492419941)

[1.4 Relationship to Other Protocols 26](#_Toc492419942)

[1.5 Prerequisites/Preconditions 27](#_Toc492419943)

[1.6 Applicability Statement 27](#_Toc492419944)

[1.7 Versioning and Capability Negotiation 27](#_Toc492419945)

[1.8 Vendor-Extensible Fields 28](#_Toc492419946)

[1.9 Standards Assignments 28](#_Toc492419947)

[2 Messages 29](#_Toc492419948)

[2.1 Transport 29](#_Toc492419949)

[2.2 Common Data Types 29](#_Toc492419950)

[2.2.1 Structures and Enumerated Types 29](#_Toc492419951)

[2.2.1.1 Basic Structures 29](#_Toc492419952)

[2.2.1.1.1 CYPHER\_BLOCK 29](#_Toc492419953)

[2.2.1.1.2 STRING 30](#_Toc492419954)

[2.2.1.1.3 LM\_OWF\_PASSWORD 30](#_Toc492419955)

[2.2.1.1.4 NT\_OWF\_PASSWORD 30](#_Toc492419956)

[2.2.1.1.5 NETLOGON\_AUTHENTICATOR 31](#_Toc492419957)

[2.2.1.2 DC Location Structures 31](#_Toc492419958)

[2.2.1.2.1 DOMAIN\_CONTROLLER\_INFOW 31](#_Toc492419959)

[2.2.1.2.2 NL\_SITE\_NAME\_ARRAY 33](#_Toc492419960)

[2.2.1.2.3 NL\_SITE\_NAME\_EX\_ARRAY 33](#_Toc492419961)

[2.2.1.2.4 NL\_SOCKET\_ADDRESS 34](#_Toc492419962)

[2.2.1.2.4.1 IPv4 Address Structure 34](#_Toc492419963)

[2.2.1.2.4.2 IPv6 Address Structure 34](#_Toc492419964)

[2.2.1.2.5 NL\_DNS\_NAME\_INFO 35](#_Toc492419965)

[2.2.1.2.6 NL\_DNS\_NAME\_INFO\_ARRAY 37](#_Toc492419966)

[2.2.1.3 Secure Channel Establishment and Maintenance Structures 37](#_Toc492419967)

[2.2.1.3.1 NL\_AUTH\_MESSAGE 37](#_Toc492419968)

[2.2.1.3.2 NL\_AUTH\_SIGNATURE 38](#_Toc492419969)

[2.2.1.3.3 NL\_AUTH\_SHA2\_SIGNATURE 39](#_Toc492419970)

[2.2.1.3.4 NETLOGON\_CREDENTIAL 41](#_Toc492419971)

[2.2.1.3.5 NETLOGON\_LSA\_POLICY\_INFO 41](#_Toc492419972)

[2.2.1.3.6 NETLOGON\_WORKSTATION\_INFO 41](#_Toc492419973)

[2.2.1.3.7 NL\_TRUST\_PASSWORD 43](#_Toc492419974)

[2.2.1.3.8 NL\_PASSWORD\_VERSION 44](#_Toc492419975)

[2.2.1.3.9 NETLOGON\_WORKSTATION\_INFORMATION 44](#_Toc492419976)

[2.2.1.3.10 NETLOGON\_ONE\_DOMAIN\_INFO 45](#_Toc492419977)

[2.2.1.3.11 NETLOGON\_DOMAIN\_INFO 46](#_Toc492419978)

[2.2.1.3.12 NETLOGON\_DOMAIN\_INFORMATION 47](#_Toc492419979)

[2.2.1.3.13 NETLOGON\_SECURE\_CHANNEL\_TYPE 48](#_Toc492419980)

[2.2.1.3.14 NETLOGON\_CAPABILITIES 48](#_Toc492419981)

[2.2.1.3.15 NL\_OSVERSIONINFO\_V1 49](#_Toc492419982)

[2.2.1.3.16 NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 50](#_Toc492419983)

[2.2.1.3.17 NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES 50](#_Toc492419984)

[2.2.1.3.18 NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 50](#_Toc492419985)

[2.2.1.3.19 NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES 51](#_Toc492419986)

[2.2.1.4 Pass-Through Authentication Structures 51](#_Toc492419987)

[2.2.1.4.1 LM\_CHALLENGE 51](#_Toc492419988)

[2.2.1.4.2 NETLOGON\_GENERIC\_INFO 51](#_Toc492419989)

[2.2.1.4.3 NETLOGON\_INTERACTIVE\_INFO 52](#_Toc492419990)

[2.2.1.4.4 NETLOGON\_SERVICE\_INFO 52](#_Toc492419991)

[2.2.1.4.5 NETLOGON\_NETWORK\_INFO 53](#_Toc492419992)

[2.2.1.4.6 NETLOGON\_LEVEL 53](#_Toc492419993)

[2.2.1.4.7 NETLOGON\_SID\_AND\_ATTRIBUTES 54](#_Toc492419994)

[2.2.1.4.8 NETLOGON\_VALIDATION\_GENERIC\_INFO2 55](#_Toc492419995)

[2.2.1.4.9 USER\_SESSION\_KEY 55](#_Toc492419996)

[2.2.1.4.10 GROUP\_MEMBERSHIP 55](#_Toc492419997)

[2.2.1.4.11 NETLOGON\_VALIDATION\_SAM\_INFO 56](#_Toc492419998)

[2.2.1.4.12 NETLOGON\_VALIDATION\_SAM\_INFO2 57](#_Toc492419999)

[2.2.1.4.13 NETLOGON\_VALIDATION\_SAM\_INFO4 58](#_Toc492420000)

[2.2.1.4.14 NETLOGON\_VALIDATION 59](#_Toc492420001)

[2.2.1.4.15 NETLOGON\_LOGON\_IDENTITY\_INFO 60](#_Toc492420002)

[2.2.1.4.16 NETLOGON\_LOGON\_INFO\_CLASS 61](#_Toc492420003)

[2.2.1.4.17 NETLOGON\_VALIDATION\_INFO\_CLASS 62](#_Toc492420004)

[2.2.1.4.18 NETLOGON Specific Access Masks 63](#_Toc492420005)

[2.2.1.5 Account Database Replication Structures 63](#_Toc492420006)

[2.2.1.5.1 NETLOGON\_DB\_CHANGE (Announcement) Message 63](#_Toc492420007)

[2.2.1.5.2 NLPR\_QUOTA\_LIMITS 65](#_Toc492420008)

[2.2.1.5.3 NETLOGON\_DELTA\_ACCOUNTS 66](#_Toc492420009)

[2.2.1.5.4 NETLOGON\_DELTA\_ALIAS 68](#_Toc492420010)

[2.2.1.5.5 NLPR\_SID\_INFORMATION 69](#_Toc492420011)

[2.2.1.5.6 NLPR\_SID\_ARRAY 69](#_Toc492420012)

[2.2.1.5.7 NETLOGON\_DELTA\_ALIAS\_MEMBER 69](#_Toc492420013)

[2.2.1.5.8 NETLOGON\_DELTA\_DELETE\_GROUP 70](#_Toc492420014)

[2.2.1.5.9 NETLOGON\_DELTA\_DELETE\_USER 70](#_Toc492420015)

[2.2.1.5.10 NETLOGON\_DELTA\_DOMAIN 71](#_Toc492420016)

[2.2.1.5.11 NETLOGON\_DELTA\_ENUM 72](#_Toc492420017)

[2.2.1.5.12 NETLOGON\_DELTA\_ENUM\_ARRAY 72](#_Toc492420018)

[2.2.1.5.13 NETLOGON\_DELTA\_GROUP 73](#_Toc492420019)

[2.2.1.5.14 NLPR\_LOGON\_HOURS 74](#_Toc492420020)

[2.2.1.5.15 NLPR\_USER\_PRIVATE\_INFO 74](#_Toc492420021)

[2.2.1.5.16 NETLOGON\_DELTA\_USER 77](#_Toc492420022)

[2.2.1.5.17 NETLOGON\_DELTA\_GROUP\_MEMBER 78](#_Toc492420023)

[2.2.1.5.18 NETLOGON\_DELTA\_ID\_UNION 78](#_Toc492420024)

[2.2.1.5.19 NETLOGON\_DELTA\_POLICY 79](#_Toc492420025)

[2.2.1.5.20 NLPR\_CR\_CIPHER\_VALUE 80](#_Toc492420026)

[2.2.1.5.21 NETLOGON\_DELTA\_SECRET 81](#_Toc492420027)

[2.2.1.5.22 NETLOGON\_DELTA\_TRUSTED\_DOMAINS 82](#_Toc492420028)

[2.2.1.5.23 NETLOGON\_RENAME\_ALIAS 83](#_Toc492420029)

[2.2.1.5.24 NETLOGON\_RENAME\_GROUP 84](#_Toc492420030)

[2.2.1.5.25 NETLOGON\_RENAME\_USER 84](#_Toc492420031)

[2.2.1.5.26 NLPR\_MODIFIED\_COUNT 85](#_Toc492420032)

[2.2.1.5.27 NETLOGON\_DELTA\_UNION 85](#_Toc492420033)

[2.2.1.5.28 NETLOGON\_DELTA\_TYPE 87](#_Toc492420034)

[2.2.1.5.29 SYNC\_STATE 88](#_Toc492420035)

[2.2.1.6 Domain Trust Structures 89](#_Toc492420036)

[2.2.1.6.1 DOMAIN\_NAME\_BUFFER 89](#_Toc492420037)

[2.2.1.6.2 DS\_DOMAIN\_TRUSTSW 89](#_Toc492420038)

[2.2.1.6.3 NETLOGON\_TRUSTED\_DOMAIN\_ARRAY 92](#_Toc492420039)

[2.2.1.6.4 NL\_GENERIC\_RPC\_DATA 92](#_Toc492420040)

[2.2.1.7 Administrative Services Structures 92](#_Toc492420041)

[2.2.1.7.1 NETLOGON\_CONTROL\_DATA\_INFORMATION 92](#_Toc492420042)

[2.2.1.7.2 NETLOGON\_INFO\_1 93](#_Toc492420043)

[2.2.1.7.3 NETLOGON\_INFO\_2 94](#_Toc492420044)

[2.2.1.7.4 NETLOGON\_INFO\_3 95](#_Toc492420045)

[2.2.1.7.5 NETLOGON\_INFO\_4 96](#_Toc492420046)

[2.2.1.7.6 NETLOGON\_CONTROL\_QUERY\_INFORMATION 96](#_Toc492420047)

[2.2.1.8 Obsolete Structures 97](#_Toc492420048)

[2.2.1.8.1 NETLOGON\_VALIDATION\_UAS\_INFO 97](#_Toc492420049)

[2.2.1.8.2 NETLOGON\_LOGOFF\_UAS\_INFO 97](#_Toc492420050)

[2.2.1.8.3 UAS\_INFO\_0 97](#_Toc492420051)

[2.2.1.8.4 NETLOGON\_DUMMY1 97](#_Toc492420052)

[2.3 Directory Service Schema Elements Used by the Netlogon Remote Protocol 98](#_Toc492420053)

[3 Protocol Details 99](#_Toc492420054)

[3.1 Netlogon Common Authentication Details 100](#_Toc492420055)

[3.1.1 Abstract Data Model 100](#_Toc492420056)

[3.1.2 Timers 102](#_Toc492420057)

[3.1.3 Initialization 102](#_Toc492420058)

[3.1.4 Message Processing Events and Sequencing Rules 102](#_Toc492420059)

[3.1.4.1 Session-Key Negotiation 102](#_Toc492420060)

[3.1.4.2 Netlogon Negotiable Options 104](#_Toc492420061)

[3.1.4.3 Session-Key Computation 106](#_Toc492420062)

[3.1.4.3.1 AES Session-Key 106](#_Toc492420063)

[3.1.4.3.2 Strong-key Session-Key 106](#_Toc492420064)

[3.1.4.3.3 DES Session-Key 107](#_Toc492420065)

[3.1.4.4 Netlogon Credential Computation 107](#_Toc492420066)

[3.1.4.4.1 AES Credential 107](#_Toc492420067)

[3.1.4.4.2 DES Credential 107](#_Toc492420068)

[3.1.4.5 Netlogon Authenticator Computation and Verification 108](#_Toc492420069)

[3.1.4.6 Calling Methods Requiring Session-Key Establishment 109](#_Toc492420070)

[3.1.4.7 Calling Methods Not Requiring Session-Key Establishment 110](#_Toc492420071)

[3.1.4.8 Determining If the Implementation Is Running on a Domain Controller 111](#_Toc492420072)

[3.1.4.9 Determining if a Request is for the Current Domain 111](#_Toc492420073)

[3.1.4.10 Client Domain Controller Location 111](#_Toc492420074)

[3.1.5 Timer Events 111](#_Toc492420075)

[3.1.6 Other Local Events 111](#_Toc492420076)

[3.2 Pass-Through Authentication Details 111](#_Toc492420077)

[3.2.1 Abstract Data Model 112](#_Toc492420078)

[3.2.2 Timers 112](#_Toc492420079)

[3.2.3 Initialization 112](#_Toc492420080)

[3.2.4 Message Processing Events and Sequencing Rules 112](#_Toc492420081)

[3.2.4.1 Generic Pass-Through 112](#_Toc492420082)

[3.2.5 Timer Events 113](#_Toc492420083)

[3.2.6 Other Local Events 113](#_Toc492420084)

[3.3 Netlogon as a Security Support Provider 113](#_Toc492420085)

[3.3.1 Abstract Data Model 113](#_Toc492420086)

[3.3.2 Timers 114](#_Toc492420087)

[3.3.3 Initialization 114](#_Toc492420088)

[3.3.4 Message Processing Events and Sequencing Rules 114](#_Toc492420089)

[3.3.4.1 The NL\_AUTH\_MESSAGE Token 114](#_Toc492420090)

[3.3.4.1.1 Generating an Initial NL\_AUTH\_MESSAGE Token 114](#_Toc492420091)

[3.3.4.1.2 Receiving an Initial NL\_AUTH\_MESSAGE Token 115](#_Toc492420092)

[3.3.4.1.3 Generating a Return NL\_AUTH\_MESSAGE Token 115](#_Toc492420093)

[3.3.4.1.4 Receiving a Return NL\_AUTH\_MESSAGE Token 115](#_Toc492420094)

[3.3.4.2 The Netlogon Signature Token 116](#_Toc492420095)

[3.3.4.2.1 Generating a Client Netlogon Signature Token 116](#_Toc492420096)

[3.3.4.2.2 Receiving a Client Netlogon Signature Token 118](#_Toc492420097)

[3.3.4.2.3 Generating a Server Netlogon Signature Token 120](#_Toc492420098)

[3.3.4.2.4 Receiving a Server Netlogon Signature Token 121](#_Toc492420099)

[3.3.5 Timer Events 121](#_Toc492420100)

[3.3.6 Other Local Events 121](#_Toc492420101)

[3.4 Netlogon Client Details 122](#_Toc492420102)

[3.4.1 Abstract Data Model 122](#_Toc492420103)

[3.4.2 Timers 123](#_Toc492420104)

[3.4.3 Initialization 123](#_Toc492420105)

[3.4.4 Higher-Layer Triggered Events 124](#_Toc492420106)

[3.4.5 Message Processing Events and Sequencing Rules 124](#_Toc492420107)

[3.4.5.1 DC Location Methods 124](#_Toc492420108)

[3.4.5.1.1 Calling DsrGetDcNameEx2 124](#_Toc492420109)

[3.4.5.1.2 Calling DsrGetDcNameEx 124](#_Toc492420110)

[3.4.5.1.3 Calling DsrGetDcName 124](#_Toc492420111)

[3.4.5.1.4 Calling NetrGetDCName 125](#_Toc492420112)

[3.4.5.1.5 Calling NetrGetAnyDCName 125](#_Toc492420113)

[3.4.5.1.6 Calling DsrGetSiteName 125](#_Toc492420114)

[3.4.5.1.7 Calling DsrGetDcSiteCoverageW 125](#_Toc492420115)

[3.4.5.1.8 Calling DsrAddressToSiteNamesW 125](#_Toc492420116)

[3.4.5.1.9 Calling DsrAddressToSiteNamesExW 125](#_Toc492420117)

[3.4.5.1.10 Calling DsrDeregisterDnsHostRecords 125](#_Toc492420118)

[3.4.5.1.11 Calling DsrUpdateReadOnlyServerDnsRecords 125](#_Toc492420119)

[3.4.5.2 Secure Channel Establishment and Maintenance Methods 125](#_Toc492420120)

[3.4.5.2.1 Calling NetrServerReqChallenge 125](#_Toc492420121)

[3.4.5.2.2 Calling NetrServerAuthenticate3 125](#_Toc492420122)

[3.4.5.2.3 Calling NetrServerAuthenticate2 126](#_Toc492420123)

[3.4.5.2.4 Calling NetrServerAuthenticate 126](#_Toc492420124)

[3.4.5.2.5 Calling NetrServerPasswordSet2 126](#_Toc492420125)

[3.4.5.2.6 Calling NetrServerPasswordSet 127](#_Toc492420126)

[3.4.5.2.7 Calling NetrServerPasswordGet 128](#_Toc492420127)

[3.4.5.2.8 Calling NetrServerTrustPasswordsGet 128](#_Toc492420128)

[3.4.5.2.9 Calling NetrLogonGetDomainInfo 128](#_Toc492420129)

[3.4.5.2.10 Calling NetrLogonGetCapabilities 128](#_Toc492420130)

[3.4.5.2.11 Calling NetrChainSetClientAttributes 129](#_Toc492420131)

[3.4.5.3 Pass-Through Authentication Methods 129](#_Toc492420132)

[3.4.5.3.1 Setting ConnectionStatus 129](#_Toc492420133)

[3.4.5.3.2 Calling NetrLogonSamLogonEx 129](#_Toc492420134)

[3.4.5.3.3 Calling NetrLogonSamLogonWithFlags 130](#_Toc492420135)

[3.4.5.3.4 Calling NetrLogonSamLogon 131](#_Toc492420136)

[3.4.5.3.5 Calling NetrLogonSamLogoff 132](#_Toc492420137)

[3.4.5.4 Account Database Replication Methods 132](#_Toc492420138)

[3.4.5.4.1 Calling NetrDatabaseDeltas 132](#_Toc492420139)

[3.4.5.4.2 Calling NetrDatabaseSync2 132](#_Toc492420140)

[3.4.5.4.3 Calling NetrDatabaseSync 133](#_Toc492420141)

[3.4.5.4.4 Calling NetrDatabaseRedo 133](#_Toc492420142)

[3.4.5.5 Domain Trusts Methods 134](#_Toc492420143)

[3.4.5.5.1 Calling DsrEnumerateDomainTrusts 134](#_Toc492420144)

[3.4.5.5.2 Calling NetrEnumerateTrustedDomainsEx 134](#_Toc492420145)

[3.4.5.5.3 Calling NetrEnumerateTrustedDomains 134](#_Toc492420146)

[3.4.5.5.4 Calling NetrGetForestTrustInformation 134](#_Toc492420147)

[3.4.5.5.5 Calling DsrGetForestTrustInformation 134](#_Toc492420148)

[3.4.5.5.6 Calling NetrServerGetTrustInfo 134](#_Toc492420149)

[3.4.5.6 Message Protection Methods 135](#_Toc492420150)

[3.4.5.6.1 Calling NetrLogonGetTrustRid 135](#_Toc492420151)

[3.4.5.6.2 Calling NetrLogonComputeServerDigest 135](#_Toc492420152)

[3.4.5.6.3 Calling NetrLogonComputeClientDigest 135](#_Toc492420153)

[3.4.5.6.4 Calling NetrLogonSendToSam 135](#_Toc492420154)

[3.4.5.6.5 Calling NetrLogonSetServiceBits 135](#_Toc492420155)

[3.4.5.6.6 Calling NetrLogonGetTimeServiceParentDomain 135](#_Toc492420156)

[3.4.5.7 Administrative Services Methods 136](#_Toc492420157)

[3.4.5.7.1 Calling NetrLogonControl2Ex 136](#_Toc492420158)

[3.4.5.7.2 Calling NetrLogonControl2 136](#_Toc492420159)

[3.4.5.7.3 Calling NetrLogonControl 136](#_Toc492420160)

[3.4.5.8 Obsolete Methods 136](#_Toc492420161)

[3.4.5.8.1 Calling NetrLogonUasLogon 136](#_Toc492420162)

[3.4.5.8.2 Calling NetrLogonUasLogoff 136](#_Toc492420163)

[3.4.5.8.3 Calling NetrAccountDeltas 136](#_Toc492420164)

[3.4.5.8.4 Calling NetrAccountSync 136](#_Toc492420165)

[3.4.6 Timer Events 136](#_Toc492420166)

[3.4.6.1 Timer Expiry on domainControllerCacheTimer 136](#_Toc492420167)

[3.4.7 Other Local Events 137](#_Toc492420168)

[3.5 Netlogon Server Details 137](#_Toc492420169)

[3.5.1 Abstract Data Model 137](#_Toc492420170)

[3.5.2 Timers 140](#_Toc492420171)

[3.5.3 Initialization 140](#_Toc492420172)

[3.5.4 Message Processing Events and Sequencing Rules 141](#_Toc492420173)

[3.5.4.1 RPC Binding Handles for Netlogon Methods 146](#_Toc492420174)

[3.5.4.2 Determining client privileges 147](#_Toc492420175)

[3.5.4.3 DC Location Methods 147](#_Toc492420176)

[3.5.4.3.1 DsrGetDcNameEx2 (Opnum 34) 147](#_Toc492420177)

[3.5.4.3.2 DsrGetDcNameEx (Opnum 27) 157](#_Toc492420178)

[3.5.4.3.3 DsrGetDcName (Opnum 20) 158](#_Toc492420179)

[3.5.4.3.4 NetrGetDCName (Opnum 11) 158](#_Toc492420180)

[3.5.4.3.5 NetrGetAnyDCName (Opnum 13) 159](#_Toc492420181)

[3.5.4.3.6 DsrGetSiteName (Opnum 28) 159](#_Toc492420182)

[3.5.4.3.7 DsrGetDcSiteCoverageW (Opnum 38) 160](#_Toc492420183)

[3.5.4.3.8 DsrAddressToSiteNamesW (Opnum 33) 161](#_Toc492420184)

[3.5.4.3.9 DsrAddressToSiteNamesExW (Opnum 37) 162](#_Toc492420185)

[3.5.4.3.10 DsrDeregisterDnsHostRecords (Opnum 41) 162](#_Toc492420186)

[3.5.4.3.11 DsrUpdateReadOnlyServerDnsRecords (Opnum 48) 163](#_Toc492420187)

[3.5.4.4 Secure Channel Establishment and Maintenance Methods 164](#_Toc492420188)

[3.5.4.4.1 NetrServerReqChallenge (Opnum 4) 165](#_Toc492420189)

[3.5.4.4.2 NetrServerAuthenticate3 (Opnum 26) 165](#_Toc492420190)

[3.5.4.4.3 NetrServerAuthenticate2 (Opnum 15) 167](#_Toc492420191)

[3.5.4.4.4 NetrServerAuthenticate (Opnum 5) 168](#_Toc492420192)

[3.5.4.4.5 NetrServerPasswordSet2 (Opnum 30) 168](#_Toc492420193)

[3.5.4.4.6 NetrServerPasswordSet (Opnum 6) 169](#_Toc492420194)

[3.5.4.4.7 NetrServerPasswordGet (Opnum 31) 170](#_Toc492420195)

[3.5.4.4.8 NetrServerTrustPasswordsGet (Opnum 42) 172](#_Toc492420196)

[3.5.4.4.9 NetrLogonGetDomainInfo (Opnum 29) 173](#_Toc492420197)

[3.5.4.4.10 NetrLogonGetCapabilities (Opnum 21) 175](#_Toc492420198)

[3.5.4.4.11 NetrChainSetClientAttributes (Opnum 49) 176](#_Toc492420199)

[3.5.4.5 Pass-Through Authentication Methods 177](#_Toc492420200)

[3.5.4.5.1 NetrLogonSamLogonEx (Opnum 39) 177](#_Toc492420201)

[3.5.4.5.2 NetrLogonSamLogonWithFlags (Opnum 45) 180](#_Toc492420202)

[3.5.4.5.3 NetrLogonSamLogon (Opnum 2) 182](#_Toc492420203)

[3.5.4.5.4 NetrLogonSamLogoff (Opnum 3) 182](#_Toc492420204)

[3.5.4.6 Account Database Replication Methods 184](#_Toc492420205)

[3.5.4.6.1 NetrDatabaseDeltas (Opnum 7) 184](#_Toc492420206)

[3.5.4.6.2 NetrDatabaseSync2 (Opnum 16) 185](#_Toc492420207)

[3.5.4.6.3 NetrDatabaseSync (Opnum 8) 188](#_Toc492420208)

[3.5.4.6.4 NetrDatabaseRedo (Opnum 17) 188](#_Toc492420209)

[3.5.4.7 Domain Trust Methods 190](#_Toc492420210)

[3.5.4.7.1 DsrEnumerateDomainTrusts (Opnum 40) 190](#_Toc492420211)

[3.5.4.7.2 NetrEnumerateTrustedDomainsEx (Opnum 36) 192](#_Toc492420212)

[3.5.4.7.3 NetrEnumerateTrustedDomains (Opnum 19) 193](#_Toc492420213)

[3.5.4.7.4 NetrGetForestTrustInformation (Opnum 44) 194](#_Toc492420214)

[3.5.4.7.5 DsrGetForestTrustInformation (Opnum 43) 195](#_Toc492420215)

[3.5.4.7.6 NetrServerGetTrustInfo (Opnum 46) 199](#_Toc492420216)

[3.5.4.8 Message Protection Methods 201](#_Toc492420217)

[3.5.4.8.1 NetrLogonGetTrustRid (Opnum 23) 201](#_Toc492420218)

[3.5.4.8.2 NetrLogonComputeServerDigest (Opnum 24) 202](#_Toc492420219)

[3.5.4.8.3 NetrLogonComputeClientDigest (Opnum 25) 203](#_Toc492420220)

[3.5.4.8.4 NetrLogonSendToSam (Opnum 32) 204](#_Toc492420221)

[3.5.4.8.5 NetrLogonSetServiceBits (Opnum 22) 205](#_Toc492420222)

[3.5.4.8.6 NetrLogonGetTimeServiceParentDomain (Opnum 35) 207](#_Toc492420223)

[3.5.4.9 Administrative Services Methods 208](#_Toc492420224)

[3.5.4.9.1 NetrLogonControl2Ex (Opnum 18) 208](#_Toc492420225)

[3.5.4.9.2 NetrLogonControl2 (Opnum 14) 213](#_Toc492420226)

[3.5.4.9.3 NetrLogonControl (Opnum 12) 214](#_Toc492420227)

[3.5.4.10 Obsolete Methods 214](#_Toc492420228)

[3.5.4.10.1 NetrLogonUasLogon (Opnum 0) 214](#_Toc492420229)

[3.5.4.10.2 NetrLogonUasLogoff (Opnum 1) 214](#_Toc492420230)

[3.5.4.10.3 NetrAccountDeltas (Opnum 9) 215](#_Toc492420231)

[3.5.4.10.4 NetrAccountSync (Opnum 10) 215](#_Toc492420232)

[3.5.5 Timer Events 215](#_Toc492420233)

[3.5.6 Other Local Events 215](#_Toc492420234)

[3.6 Netlogon NT Replication Details 215](#_Toc492420235)

[3.6.1 Abstract Data Model 217](#_Toc492420236)

[3.6.2 Timers 218](#_Toc492420237)

[3.6.3 Initialization 218](#_Toc492420238)

[3.6.4 Message Processing Events and Sequencing Rules 218](#_Toc492420239)

[3.6.4.1 Message Processing on PDC 218](#_Toc492420240)

[3.6.4.2 Message Processing on BDC 220](#_Toc492420241)

[3.6.5 Timer Events 220](#_Toc492420242)

[3.6.5.1 Timer Events on PDC 220](#_Toc492420243)

[3.6.5.2 Timer Events on BDC 221](#_Toc492420244)

[3.6.5.2.1 Full Synchronization 221](#_Toc492420245)

[3.6.5.2.2 Partial Synchronization 221](#_Toc492420246)

[3.6.6 Other Local Events 222](#_Toc492420247)

[4 Protocol Examples 223](#_Toc492420248)

[4.1 NetrLogonSamLogon with Secure Channel 223](#_Toc492420249)

[4.2 Cryptographic Values for Session Key Validation 228](#_Toc492420250)

[4.2.1 ASCII MD4 Testing 229](#_Toc492420251)

[4.2.2 UNICODE MD4 Testing 229](#_Toc492420252)

[5 Security Considerations 230](#_Toc492420253)

[5.1 Security Considerations for Implementers 230](#_Toc492420254)

[5.2 Index of Security Parameters 231](#_Toc492420255)

[6 Appendix A: Full IDL 232](#_Toc492420256)

[7 Appendix B: Product Behavior 256](#_Toc492420257)

[8 Change Tracking 276](#_Toc492420258)

[9 Index 277](#_Toc492420259)

# Introduction

The Netlogon Remote Protocol is a [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) interface that is used for user and machine authentication on domain-based networks.

The Netlogon Remote Protocol RPC interface is also used to replicate the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) for [**backup domain controllers (BDCs)**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3).

The Netlogon Remote Protocol is used to maintain [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) relationships from the members of a domain to the [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), among DCs for a domain, and between DCs across domains. This RPC interface is used to discover and manage these relationships.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

## Glossary

This document uses the following terms:

**Active Directory**: A general-purpose network [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) also refers to the Windows implementation of a [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) stores information about a variety of objects in the network. User accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) describes both forms. For more information, see [[MS-AUTHSOD]](%5bMS-AUTHSOD%5d.pdf#Section_953d700a57cb4cf7b0c3a64f34581cc9) section 1.1.1.5.2, Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Kerberos, and [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700).

**Advanced Encryption Standard (AES)**: A block cipher that supersedes the Data Encryption Standard (DES). AES can be used to protect electronic data. The AES algorithm can be used to encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. AES is used in symmetric-key cryptography, meaning that the same key is used for the encryption and decryption operations. It is also a block cipher, meaning that it operates on fixed-size blocks of plaintext and ciphertext, and requires the size of the plaintext as well as the ciphertext to be an exact multiple of this block size. AES is also known as the Rijndael symmetric encryption algorithm [[FIPS197]](https://go.microsoft.com/fwlink/?LinkId=89870).

**alias**: A group that is local to a particular machine (as opposed to a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) that has security permissions and settings for the entire [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca)).

**authentication level**: A numeric value indicating the level of authentication or message protection that [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) will apply to a specific message exchange. For more information, see [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 13.1.2.1 and [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15).

**authenticator**: When used in reference to the Netlogon Protocol, the data stored in the NETLOGON\_AUTHENTICATOR structure.

**authoritative response**: An authoritative response is one in which the server has all necessary resources to service the caller's request. If some of the resources are temporarily unavailable, then the server will indicate that its response is not authoritative. When a server does not return an authoritative response, it is reasonable for the caller to retry the request at another server. The reasons why a request is non-authoritative are always implementation-specific and could include any failure of the server to allocate necessary resources.

**backup domain controller (BDC)**: A [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) that receives a copy of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) directory database from the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). This copy is synchronized periodically and automatically with the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). BDCs also authenticate user logons and can be promoted to function as the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). There is only one [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) or [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) emulator in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), and the rest are [**backup domain controllers**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3).

**binary large object (BLOB)**: A collection of binary data stored as a single entity in a database.

**binding handle**: A data structure that represents the logical connection between a client and a server.

**checked build**: A special build of an operating system that contains fewer compiler optimizations and more debugging checks than a production environment build. The purpose of the checked build is to make identifying and diagnosing operating system–level problems easier. For more information, see [[MSDN-CHKBLD]](https://go.microsoft.com/fwlink/?LinkId=105832).

**client challenge**: A 64-bit [**nonce**](#gt_001c0e40-0980-417d-853c-f7cb34ba6d3b) generated on the client side.

**computer name**: The [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or NetBIOS name.

**computer object**: An object of class computer. A [**computer object**](#gt_d8e8f5a7-db85-40a8-98ed-1abab2237b82) is a [**security principal**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409) object; the principal is the operating system running on the computer. The shared secret allows the operating system running on the computer to authenticate itself independently of any user running on the system. See [**security principal**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409).

**credential**: Previously established, authentication data that is used by a security principal to establish its own identity. When used in reference to the Netlogon Protocol, it is the data that is stored in the NETLOGON\_CREDENTIAL structure.

**database**: For the purposes of the Netlogon RPC, a database is a collection of user accounts, machine accounts, aliases, groups, and policies, managed by a component. The database, or the component managing the database, must expose a mechanism to enable Netlogon to gather changes from and apply changes to the database. Additionally, it must export a database serial number in order to track changes for efficient replication.

**database serial number**: A numeric value that is incremented each time a database transaction is applied to the database.

**decryption**: In cryptography, the process of transforming encrypted information to its original clear text form.

**delta**: One of a set of possible changes that can be made to a [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15).

**direct trust**: A type of authentication functionality in which one [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) accepts another [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) as an authoritative source to provide object authentication and other [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) services for that other [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). For example, if a [**direct trust**](#gt_e03f25c6-dd6e-43df-83e2-98f89bcc50d9) is established from [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), DOMAIN-A, to [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), DOMAIN-B, DOMAIN-A trusts DOMAIN-B. If a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), DOMAIN-A, must authenticate an object, such as a user account, from a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), DOMAIN-B, DOMAIN-A requests that DOMAIN-B authenticate the user account, and DOMAIN-A will treat the response from DOMAIN-B as reliable.

**directory service (DS)**: A service that stores and organizes information about a computer network's users and network shares, and that allows network administrators to manage users' access to the shares. See also [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90).

**domain**: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) and host a member list that identifies all members of the domain, as well as optionally hosting the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

**domain account**: A stored set of attributes representing a principal used to authenticate a user or machine to an [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) domain.

**domain controller (DC)**: The service, running on a server, that implements [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90), or the server hosting this service. The service hosts the data store for objects and interoperates with other [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) to ensure that a local change to an object replicates correctly across all [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). When [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is operating as Active Directory Domain Services (AD DS), the [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) contains full NC replicas of the configuration naming context (config NC), schema naming context (schema NC), and one of the domain NCs in its [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). If the AD DS [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) is a global catalog server (GC server), it contains partial NC replicas of the remaining domain NCs in its [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). For more information, see [MS-AUTHSOD] section 1.1.1.5.2 and [MS-ADTS]. When [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is operating as Active Directory Lightweight Directory Services (AD LDS), several AD LDS [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) can run on one server. When [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) is operating as AD DS, only one AD DS [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) can run on one server. However, several AD LDS [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) can coexist with one AD DS [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) on one server. The AD LDS [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) contains full NC replicas of the config NC and the schema NC in its [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). The domain controller is the server side of Authentication Protocol Domain Support [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e).

**domain local group**: An [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) group that allows user objects, global groups, and universal groups from any [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) as members. It can additionally include, and be a member of, other [**domain local groups**](#gt_32226492-3c8c-4a99-a0d1-f27aaeec3c97) from within its [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). A group object g is a [**domain local group**](#gt_32226492-3c8c-4a99-a0d1-f27aaeec3c97) if and only if GROUP\_TYPE\_RESOURCE\_GROUP is present in g!groupType; see [MS-ADTS] section 2.2.12, "Group Type Flags". A security-enabled [**domain local group**](#gt_32226492-3c8c-4a99-a0d1-f27aaeec3c97) is valid for inclusion within access control lists (ACLs) from its own [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). If a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) is in [**mixed mode**](#gt_06c1c70e-f2c6-4efd-bff8-474409e69660), then a security-enabled [**domain local group**](#gt_32226492-3c8c-4a99-a0d1-f27aaeec3c97) in that [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) allows only user objects as members.

**domain member (member machine)**: A machine that is joined to a domain by sharing a secret between the machine and the domain.

**domain name**: A domain name or a [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) that identifies a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**Domain Name System (DNS)**: A hierarchical, distributed database that contains mappings of domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

**domain tree**: A set of [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that are arranged hierarchically, typically following an accompanying DNS hierarchy, with trusts between parents and children. An example [**domain tree**](#gt_e2c071f1-5977-4749-868f-6c5a04929476) might be a.example.com, b.example.com, and example.com; domain A and domain B each trust example.com but do not trust each other directly. They will have a transitive trust relationship through example.com.

**dynamic endpoint**: A network-specific server address that is requested and assigned at run time. For more information, see [C706].

**encryption key**: One of the input parameters to an encryption algorithm. Generally speaking, an encryption algorithm takes as input a clear-text message and a key, and results in a cipher-text message. The corresponding [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) algorithm takes a cipher-text message, and the key, and results in the original clear-text message.

**endpoint**: A network-specific address of a remote procedure call (RPC) server process for remote procedure calls. The actual name and type of the endpoint depends on the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) protocol sequence that is being used. For example, for RPC over TCP (RPC Protocol Sequence ncacn\_ip\_tcp), an endpoint might be TCP port 1025. For RPC over Server Message Block (RPC Protocol Sequence ncacn\_np), an endpoint might be the name of a named pipe. For more information, see [C706].

**enterprise network**: The network of computer systems in an organization, such as a corporation. An enterprise can span geographical locations and often includes a variety of computer types, operating systems, protocols, and network architectures.

**forest**: One or more [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that share a common schema and trust each other transitively. An organization can have multiple [**forests**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). A [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) establishes the security and administrative boundary for all the objects that reside within the [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that belong to the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). In contrast, a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) establishes the administrative boundary for managing objects, such as users, groups, and computers. In addition, each [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) has individual security policies and trust relationships with other [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**forest trust**: A type of [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) where the trusted party is a [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62), which means that all [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) in that [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) are trusted.

**forest trust information**: Information about namespaces, [**domain names**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c), and [**security identifiers (SIDs)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) owned by a trusted [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62).

**full database synchronization**: A mechanism for synchronizing an entire database record set on a particular replication partner.

**fully qualified domain name (FQDN)**: (1) An unambiguous domain name that gives an absolute location in the [**Domain Name System's (DNS)**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) hierarchy tree, as defined in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) section 3.1 and [[RFC2181]](https://go.microsoft.com/fwlink/?LinkId=127732) section 11.

(2) In [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90), a [**fully qualified domain name (FQDN) (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) that identifies a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**global catalog (GC)**: A unified partial view of multiple [**naming contexts (NCs)**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) in a distributed partitioned directory. The [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) directory service [**GC**](#gt_4f5d605a-7b3f-4db7-8c21-b146856d7169) is implemented by GC servers. The definition of [**global catalog**](#gt_4f5d605a-7b3f-4db7-8c21-b146856d7169) is specified in [MS-ADTS] section 3.1.1.1.8.

**globally unique identifier (GUID)**: A term used interchangeably with [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [[RFC4122]](https://go.microsoft.com/fwlink/?LinkId=90460) or [C706] must be used for generating the [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). See also [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3).

**group**: A collection of objects that can be treated as a whole.

**Hash-based Message Authentication Code (HMAC)**: A mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function (for example, MD5 and SHA-1) in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

**interactive logon**: A software method in which the account information and credentials input by the user interactively are authenticated by a [**server**](#gt_434b0234-e970-4e8c-bdfa-e16a30d96703) or [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**Interface Definition Language (IDL)**: The International Standards Organization (ISO) standard language for specifying the interface for remote procedure calls. For more information, see [C706] section 4.

**Key Distribution Center (KDC)**: The Kerberos service that implements the authentication and ticket granting services specified in the Kerberos protocol. The service runs on computers selected by the administrator of the realm or domain; it is not present on every machine on the network. It must have access to an account database for the realm that it serves. [**KDCs**](#gt_6e5aafba-6b66-4fdd-872e-844f142af287) are integrated into the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) role. It is a network service that supplies tickets to clients for use in authenticating to services.

**Local Security Authority (LSA)**: A protected subsystem that authenticates and logs users onto the local system. [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) also maintains information about all aspects of local security on a system, collectively known as the local security policy of the system.

**Local Security Authority (LSA) database**: A Microsoft-specific terminology for the part of the user account database containing account privilege information (such as specific account rights) and domain security policy information.

**mailslot**: A mechanism for one-way interprocess communications (IPC). For more information, see [[MSLOT]](https://go.microsoft.com/fwlink/?LinkId=90218) and [[MS-MAIL]](%5bMS-MAIL%5d.pdf#Section_8ea19aa46e5a4aedb6280b5cd75a1ab9).

**mixed mode**: A state of an [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that supports [**domain controllers (DCs)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) running Windows NT Server 4.0 operating system. Mixed mode does not allow organizations to take advantage of new [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) features such as universal groups, nested group membership, and interdomain group membership. See also native mode.

**naming context (NC)**: An [**NC**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) is a set of objects organized as a tree. It is referenced by a DSName. The DN of the DSName is the distinguishedName attribute of the tree root. The [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) of the DSName is the objectGUID attribute of the tree root. The [**security identifier (SID)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) of the DSName, if present, is the objectSid attribute of the tree root; for Active Directory Domain Services (AD DS), the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) is present if and only if the [**NC**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) is a domain naming context (domain NC). [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) supports organizing several [**NCs**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) into a tree structure.

**NetBIOS name**: A 16-byte address that is used to identify a NetBIOS resource on the network. For more information, see [[RFC1001]](https://go.microsoft.com/fwlink/?LinkId=90260) and [[RFC1002]](https://go.microsoft.com/fwlink/?LinkId=90261).

**Netlogon**: In a Windows NT operating system-compatible network security environment, the component responsible for synchronization and maintenance functions between a [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) and backup domain controllers (BDC). [**Netlogon**](#gt_70771a5a-04a3-447d-981b-e03098808c32) is a precursor to the directory replication server (DRS) protocol.

**network logon**: A software method in which the account information and credentials previously supplied by the user as part of an interactive logon are used again to log the user onto another network resource.

**nonce**: A number that is used only once. This is typically implemented as a random number large enough that the probability of number reuse is extremely small. A nonce is used in authentication protocols to prevent replay attacks. For more information, see [[RFC2617]](https://go.microsoft.com/fwlink/?LinkId=90373).

**NT LAN Manager (NTLM)**: An authentication protocol that is based on a challenge-response sequence for authentication. For more information, see [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4).

**one-way function (OWF)**: The calculation of a hash of the password using the Rivest-Shamir-Adleman (RSA) MD4 function. [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) is used to refer to the resulting value of the hash operation.

**opnum**: An operation number or numeric identifier that is used to identify a specific [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) method or a method in an interface. For more information, see [C706] section 12.5.2.12 or [MS-RPCE].

**original equipment manufacturer (OEM) character set**: A character encoding used where the mappings between characters is dependent upon the code page configured on the machine, typically by the manufacturer.

**partial database synchronization**: A mechanism for synchronizing a set of database records on a particular replication partner.

**primary domain**: A [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) (identified by a [**security identifier (SID)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d)) that the server is joined to. For a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) is that of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) itself.

**primary domain controller (PDC)**: A [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) designated to track changes made to the accounts of all computers on a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). It is the only computer to receive these changes directly, and is specialized so as to ensure consistency and to eliminate the potential for conflicting entries in the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) database. A [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) has only one [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d).

**principal**: An authenticated entity that initiates a message or channel in a distributed system.

**privilege**: The right of a user to perform system-related operations, such as debugging the system. A user's authorization context specifies what privileges are held by that user.

**RC4**: A variable key-length symmetric encryption algorithm. For more information, see [[SCHNEIER]](https://go.microsoft.com/fwlink/?LinkId=817338) section 17.1.

**read-only domain controller (RODC)**: A [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) that does not accept originating updates. Additionally, an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) does not perform outbound replication. An RODC cannot be the primary domain controller (PDC) for its domain.

**relative identifier (RID)**: The last item in the series of SubAuthority values in a [**security identifier (SID)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) [[SIDD]](https://go.microsoft.com/fwlink/?LinkId=90516). It distinguishes one account or group from all other accounts and groups in the domain. No two accounts or groups in any domain share the same RID.

**remote procedure call (RPC)**: A context-dependent term commonly overloaded with three meanings. Note that much of the industry literature concerning RPC technologies uses this term interchangeably for any of the three meanings. Following are the three definitions: (\*) The runtime environment providing remote procedure call facilities. The preferred usage for this meaning is "RPC runtime". (\*) The pattern of request and response message exchange between two parties (typically, a client and a server). The preferred usage for this meaning is "RPC exchange". (\*) A single message from an exchange as defined in the previous definition. The preferred usage for this term is "RPC message". For more information about RPC, see [C706].

**RPC protocol sequence**: A character string that represents a valid combination of a [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) protocol, a network layer protocol, and a transport layer protocol, as described in [C706] and [MS-RPCE].

**RPC transport**: The underlying network services used by the remote procedure call (RPC) runtime for communications between network nodes. For more information, see [C706] section 2.

**secret key**: A symmetric encryption key shared by two entities, such as between a user and the [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), with a long lifetime. A password is a common example of a secret key. When used in a context that implies Kerberos only, a principal's secret key.

**secure channel**: An authenticated [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) connection between two machines in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) with an established [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) used for signing and encrypting [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) packets.

**Security Account Manager (SAM)**: A centrally managed service, such as Active Directory Domain Services (AD DS), that enables a server to establish a trust relationship with other authorized servers. The SAM also maintains information about domains and security principals, and provides client-to-server information by using several available standards for access control lists (ACLs).

**security account manager (SAM) built-in database**: The part of the user account database that contains account information (such as account names and passwords) for accounts and groups that are pre-created at the database installation.

**security context**: An abstract data structure that contains authorization information for a particular [**security principal**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409) in the form of a Token/Authorization Context (see [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.5.2). A server uses the authorization information in a [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) to check access to requested resources. A [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) also contains a key identifier that associates mutually established cryptographic keys, along with other information needed to perform secure communication with another security principal.

**security identifier (SID)**: An identifier for [**security principals**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409) that is used to identify an account or a group. Conceptually, the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) is composed of an account authority portion (typically a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca)) and a smaller integer representing an identity relative to the account authority, termed the [**relative identifier (RID)**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c). The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) format is specified in [MS-DTYP] section 2.4.2; a string representation of [**SIDs**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) is specified in [MS-DTYP] section 2.4.2 and [[MS-AZOD]](%5bMS-AZOD%5d.pdf#Section_5a0a0a3ec7a742e1b5f2cc8d8bd9739e) section 1.1.1.2.

**security principal**: A unique entity, also referred to as a principal, that can be authenticated by [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). It frequently corresponds to a human user, but also can be a service that offers a resource to other security principals. Other security principals might be a group, which is a set of principals. Groups are supported by [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90).

**security provider**: A pluggable security module that is specified by the protocol layer above the [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) layer, and will cause the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) layer to use this module to secure messages in a communication session with the server. The security provider is sometimes referred to as an authentication service. For more information, see [C706] and [MS-RPCE].

**security support provider (SSP)**: A dynamic-link library (DLL) that implements the [**Security Support Provider Interface (SSPI)**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) by making one or more security packages available to applications. Each security package provides mappings between an application's [**SSPI**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) function calls and an actual security model's functions. Security packages support security protocols such as Kerberos authentication and NTLM.

**Security Support Provider Interface (SSPI)**: A Windows-specific API implementation that provides the means for connected applications to call one of several security providers to establish authenticated connections and to exchange data securely over those connections. This is the Windows equivalent of Generic Security Services (GSS)-API, and the two families of APIs are on-the-wire compatible.

**server**: A computer on which the [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) server is executing.

**server challenge (SC)**: A 64-bit nonce generated on the server side.

**service principal name (SPN)**: The name a client uses to identify a service for mutual authentication. (For more information, see [[RFC1964]](https://go.microsoft.com/fwlink/?LinkId=90304) section 2.1.1.) An [**SPN**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4) consists of either two parts or three parts, each separated by a forward slash ('/'). The first part is the service class, the second part is the host name, and the third part (if present) is the service name. For example, "ldap/dc-01.fabrikam.com/fabrikam.com" is a three-part [**SPN**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4) where "ldap" is the service class name, "dc-01.fabrikam.com" is the host name, and "fabrikam.com" is the service name. See [[SPNNAMES]](https://go.microsoft.com/fwlink/?LinkId=90532) for more information about [**SPN**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4) format and composing a unique [**SPN**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4).

**session key**: A relatively short-lived symmetric key (a cryptographic key negotiated by the client and the server based on a shared secret). A [**session key's**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) lifespan is bounded by the session to which it is associated. A [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) has to be strong enough to withstand cryptanalysis for the lifespan of the session.

**shared secret**: A piece of data that is known only to the [**security principal**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409) and an authenticating authority; for example, a user and a domain controller. It is used to prove the [**principal's**](#gt_8492780e-99e2-47ba-8553-aedb8de9f9c0) identity. A password is a common example of a shared secret. Also called a "secret key".

**site**: A collection of one or more well-connected (reliable and fast) TCP/IP subnets. By defining [**sites**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) (represented by site objects) an administrator can optimize both [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) access and [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) replication with respect to the physical network. When users log in, [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) clients find [**domain controllers (DCs)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) that are in the same [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) as the user, or near the same [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) if there is no [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba). See also Knowledge Consistency Checker (KCC). For more information, see [MS-ADTS].

**sub-authentication**: Optional and additional authentication functionality, usually provided by extending an authentication algorithm.

**sub-authentication package**: An optional component that provides additional authentication functionality. If a [**sub-authentication package**](#gt_b1331d67-e2ca-45e1-af31-50f52659a0c2) is installed, the authentication package calls the [**sub-authentication package**](#gt_b1331d67-e2ca-45e1-af31-50f52659a0c2) before returning its authentication result. The request to verify by a [**sub-authentication package**](#gt_b1331d67-e2ca-45e1-af31-50f52659a0c2) is indicated by the ParameterControl field of the LogonInformation parameter (see [MS-APDS] section 3.1.5.2.1, Verifying Responses with Sub-Authentication Packages).

**transitive trust**: The state of two domains establishing trust through an intermediary domain. For example, if domain A trusts domain B, and domain B trusts domain C, then domain A can be configured to trust domain C through transitive trust.

**trust**: To accept another authority's statements for the purposes of authentication and authorization, especially in the case of a relationship between two domains. If [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) A trusts [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) B, [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) A accepts [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) B's authentication and authorization statements for [**principals**](#gt_8492780e-99e2-47ba-8553-aedb8de9f9c0) represented by security principal objects in [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) B; for example, the list of groups to which a particular user belongs. As a noun, a [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) is the relationship between two [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) described in the previous sentence.

**trusted domain object (TDO)**: A collection of properties that define a trust relationship with another domain, such as direction (outbound, inbound, or both), trust attributes, name, and security identifier of the other domain. For more information, see [MS-ADTS].

**Unicode**: A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) standard [[UNICODE5.0.0/2007]](https://go.microsoft.com/fwlink/?LinkId=154659) provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

**universally unique identifier (UUID)**: A 128-bit value. UUIDs can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) objects. UUIDs are highly likely to be unique. UUIDs are also known as [**globally unique identifiers (GUIDs)**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) and these terms are used interchangeably in the Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the UUID. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [C706] must be used for generating the UUID.

**user principal name (UPN)**: A user account name (sometimes referred to as the user logon name) and a domain name that identifies the domain in which the user account is located. This is the standard usage for logging on to a Windows domain. The format is: someone@example.com (in the form of an email address). In [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90), the userPrincipalName attribute of the account object, as described in [MS-ADTS].

**Windows Time Service (W32Time)**: A service that supports time synchronization against network and hardware time sources. For more information, see [[WTSREF]](https://go.microsoft.com/fwlink/?LinkId=90586) and [[MS-SNTP]](%5bMS-SNTP%5d.pdf#Section_8106cb73ab3a45428bc8784dd32031cc).

**writable domain controller**: A [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) that performs originating updates and outbound replication.

**MAY, SHOULD, MUST, SHOULD NOT, MUST NOT:** These terms (in all caps) are used as defined in [[RFC2119]](https://go.microsoft.com/fwlink/?LinkId=90317). All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

## References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the [Errata](https://go.microsoft.com/fwlink/?linkid=850906).

### Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com). We will assist you in finding the relevant information.

[C706] The Open Group, "DCE 1.1: Remote Procedure Call", C706, August 1997, [https://www2.opengroup.org/ogsys/catalog/c706](https://go.microsoft.com/fwlink/?LinkId=89824)

[FIPS197] FIPS PUBS, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, [http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf](https://go.microsoft.com/fwlink/?LinkId=89870)

[FIPS46-2] FIPS PUBS, "Data Encryption Standard (DES)", FIPS PUB 46-2, December 1993, [http://www.itl.nist.gov/fipspubs/fip46-2.htm](https://go.microsoft.com/fwlink/?LinkId=89871)

[FIPS81] FIPS PUBS, "DES Modes of Operation", December 1980, [http://csrc.nist.gov/publications/fips/fips81/fips81.htm](https://go.microsoft.com/fwlink/?LinkId=89874)

[MS-ADA1] Microsoft Corporation, "[Active Directory Schema Attributes A-L](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f)".

[MS-ADA2] Microsoft Corporation, "[Active Directory Schema Attributes M](%5bMS-ADA2%5d.pdf#Section_e20ebc4e528540bab3bdffcb81c2783e)".

[MS-ADA3] Microsoft Corporation, "[Active Directory Schema Attributes N-Z](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0)".

[MS-ADSC] Microsoft Corporation, "[Active Directory Schema Classes](%5bMS-ADSC%5d.pdf#Section_9abb5e97123d4da99557b353ab79b830)".

[MS-ADTS] Microsoft Corporation, "[Active Directory Technical Specification](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a)".

[MS-APDS] Microsoft Corporation, "[Authentication Protocol Domain Support](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e)".

[MS-CIFS] Microsoft Corporation, "[Common Internet File System (CIFS) Protocol](%5bMS-CIFS%5d.pdf#Section_d416ff7cc536406ea9514f04b2fd1d2b)".

[MS-DRSR] Microsoft Corporation, "[Directory Replication Service (DRS) Remote Protocol](%5bMS-DRSR%5d.pdf#Section_f977faaa673e4f66b9bf48c640241d47)".

[MS-DTYP] Microsoft Corporation, "[Windows Data Types](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2)".

[MS-ERREF] Microsoft Corporation, "[Windows Error Codes](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90)".

[MS-GPSB] Microsoft Corporation, "[Group Policy: Security Protocol Extension](%5bMS-GPSB%5d.pdf#Section_6a07a06be62847659d910d63ba47fdc0)".

[MS-LSAD] Microsoft Corporation, "[Local Security Authority (Domain Policy) Remote Protocol](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc)".

[MS-MAIL] Microsoft Corporation, "[Remote Mailslot Protocol](%5bMS-MAIL%5d.pdf#Section_8ea19aa46e5a4aedb6280b5cd75a1ab9)".

[MS-NBTE] Microsoft Corporation, "[NetBIOS over TCP (NBT) Extensions](%5bMS-NBTE%5d.pdf#Section_3461cfa83d284fa38163131bf1046fa3)".

[MS-NLMP] Microsoft Corporation, "[NT LAN Manager (NTLM) Authentication Protocol](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)".

[MS-PAC] Microsoft Corporation, "[Privilege Attribute Certificate Data Structure](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962)".

[MS-RCMP] Microsoft Corporation, "[Remote Certificate Mapping Protocol](%5bMS-RCMP%5d.pdf#Section_5462719690dd4e968c7f7520066785ba)".

[MS-RPCE] Microsoft Corporation, "[Remote Procedure Call Protocol Extensions](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15)".

[MS-RPRN] Microsoft Corporation, "[Print System Remote Protocol](%5bMS-RPRN%5d.pdf#Section_d42db7d5f14144668f470a4be14e2fc1)".

[MS-RRP] Microsoft Corporation, "[Windows Remote Registry Protocol](%5bMS-RRP%5d.pdf#Section_0fa3191dbb79490a81bd54c2601b7a78)".

[MS-SAMR] Microsoft Corporation, "[Security Account Manager (SAM) Remote Protocol (Client-to-Server)](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380)".

[MS-SAMS] Microsoft Corporation, "[Security Account Manager (SAM) Remote Protocol (Server-to-Server)](%5bMS-SAMS%5d.pdf#Section_2e785e4ed5b64ae3b479351a50830921)".

[MS-SMB] Microsoft Corporation, "[Server Message Block (SMB) Protocol](%5bMS-SMB%5d.pdf#Section_f210069c70864dc2885e861d837df688)".

[MS-SNTP] Microsoft Corporation, "[Network Time Protocol (NTP) Authentication Extensions](%5bMS-SNTP%5d.pdf#Section_8106cb73ab3a45428bc8784dd32031cc)".

[MS-WKST] Microsoft Corporation, "[Workstation Service Remote Protocol](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7)".

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987, [http://www.ietf.org/rfc/rfc1035.txt](https://go.microsoft.com/fwlink/?LinkId=90264)

[RFC1320] Rivest, R., "The MD4 Message-Digest Algorithm", RFC 1320, April 1992, [http://www.ietf.org/rfc/rfc1320.txt](https://go.microsoft.com/fwlink/?LinkId=90274)

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992, [http://www.ietf.org/rfc/rfc1321.txt](https://go.microsoft.com/fwlink/?LinkId=90275)

[RFC2104] Krawczyk, H., Bellare, M., and Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997, [http://www.ietf.org/rfc/rfc2104.txt](https://go.microsoft.com/fwlink/?LinkId=90314)

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, [http://www.rfc-editor.org/rfc/rfc2119.txt](https://go.microsoft.com/fwlink/?LinkId=90317)

[RFC2234] Crocker, D. and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997, [http://www.ietf.org/rfc/rfc2234.txt](https://go.microsoft.com/fwlink/?LinkId=90323)

[RFC2782] Gulbrandsen, A., Vixie, P., and Esibov, L., "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000, [http://www.ietf.org/rfc/rfc2782.txt](https://go.microsoft.com/fwlink/?LinkId=90381)

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and Stevens, W., "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003, [http://www.ietf.org/rfc/rfc3493.txt](https://go.microsoft.com/fwlink/?LinkId=90425)

[RFC4634] Eastlake III, D. and Hansen, T., "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006, [http://www.ietf.org/rfc/rfc4634.txt](https://go.microsoft.com/fwlink/?LinkId=90486)

[RFC791] Postel, J., Ed., "Internet Protocol: DARPA Internet Program Protocol Specification", RFC 791, September 1981, [http://www.rfc-editor.org/rfc/rfc791.txt](https://go.microsoft.com/fwlink/?LinkId=392659)

### Informative References

[LANMAN] Microsoft Corporation, "LAN Manager Authentication Level", [http://msdn.microsoft.com/en-us/library/ms814176.aspx](https://go.microsoft.com/fwlink/?LinkId=89929)

[LSAPOLICY] Microsoft Corporation, "LSA Policy", [http://msdn.microsoft.com/en-us/library/ms721831.aspx](https://go.microsoft.com/fwlink/?LinkId=89934)

[MS-ADOD] Microsoft Corporation, "[Active Directory Protocols Overview](%5bMS-ADOD%5d.pdf#Section_5ff67bf4c14548cb89cd4f5482d94664)".

[MS-GPOD] Microsoft Corporation, "[Group Policy Protocols Overview](%5bMS-GPOD%5d.pdf#Section_6e6349392ccf4412b75f0035dc05ea67)".

[NTLM] Microsoft Corporation, "Microsoft NTLM", [http://msdn.microsoft.com/en-us/library/aa378749.aspx](https://go.microsoft.com/fwlink/?LinkId=90235)

[NTSTATUSERR] Microsoft Corporation, "NTSTATUS Values", [http://msdn.microsoft.com/en-us/library/ff557697.aspx](https://go.microsoft.com/fwlink/?LinkId=90238)

[PIPE] Microsoft Corporation, "Named Pipes", [http://msdn.microsoft.com/en-us/library/aa365590.aspx](https://go.microsoft.com/fwlink/?LinkId=90247)

[SCHNEIER] Schneier, B., "Applied Cryptography, Second Edition", John Wiley and Sons, 1996, ISBN: 0471117099, [http://www.wiley.com/WileyCDA/WileyTitle/productCd-0471117099.html](https://go.microsoft.com/fwlink/?LinkId=817338)

[SIDATT] Microsoft Corporation, "TOKEN\_GROUPS", [http://msdn.microsoft.com/en-us/library/aa379624.aspx](https://go.microsoft.com/fwlink/?LinkId=90515)

[SPNNAMES] Microsoft Corporation, "Name Formats for Unique SPNs", [http://msdn.microsoft.com/en-us/library/ms677601.aspx](https://go.microsoft.com/fwlink/?LinkId=90532)

[SSPI] Microsoft Corporation, "SSPI", [http://msdn.microsoft.com/en-us/library/aa380493.aspx](https://go.microsoft.com/fwlink/?LinkId=90536)

## Overview

The Netlogon Remote Protocol is used for secure communication between machines in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) (both [**domain members**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) and [**domain controllers (DCs)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd)) and DCs. The communication is secured by using a shared [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) computed between the client and the DC that is engaged in the secure communication. The session key is computed by using a preconfigured [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) that is known to the client and the DC.

The Netlogon Remote Protocol client and server can only run on domain-joined systems, and are started during boot. When a system is unjoined from the domain, then the client and server are stopped and will not be started during boot.

The following sections describe the scenarios in which this protocol is used. It provides an overview about the general purpose of this protocol and the flow of its operations.

### Pass-Through Authentication

In a scenario where a user does an [**interactive logon**](#gt_9360639b-135c-46dc-9f9e-85728008146f) to a client machine and connects to a server, the connection is authenticated. The client and the server engage in an authentication protocol, such as NTLM (as specified in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)), which validates the user [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) and logs the user on to the server upon successful validation. This type of logon is known as [**network logon**](#gt_c020fc9f-456f-4fd0-8e25-001ef6b8acf2) because it happens over a network connection from the client to the server.

To authenticate the user, the server passes the user credentials securely to a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) of the user account. (The DC is the only entity, other than the client machine, that knows the user [**secret key**](#gt_dc4cd75d-71f9-4ceb-8938-504d0c6b2fbf); that is, the user password.) After the logon request is delivered to the DC and the DC successfully validates the credentials, the DC refers back to the server those attributes of the user account that the server can use in authorization decisions (such as granting the user access to a particular file).

It is the responsibility of the Netlogon Remote Protocol to deliver the logon request to the DC over a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) that is established from the server (acting as the secure channel client) to the DC (acting as the secure channel server). The secure channel is achieved by encrypting the communication traffic with a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) computed using a secret key (called a server's machine account password) shared by the server and the DC.

Upon successful validation of the user credentials on the DC, the Netlogon Remote Protocol delivers the user authorization attributes (referred to as user validation information) back to the server over the secure channel.

This mechanism of delegating the authentication request to a DC is called pass-through authentication, a process in which the server passes the logon request through to the DC. The following illustration depicts a process of pass-through authentication in which the authentication request is passed over a secure channel from a server in Domain A to a DC in the domain containing the user account, in this case also Domain A.

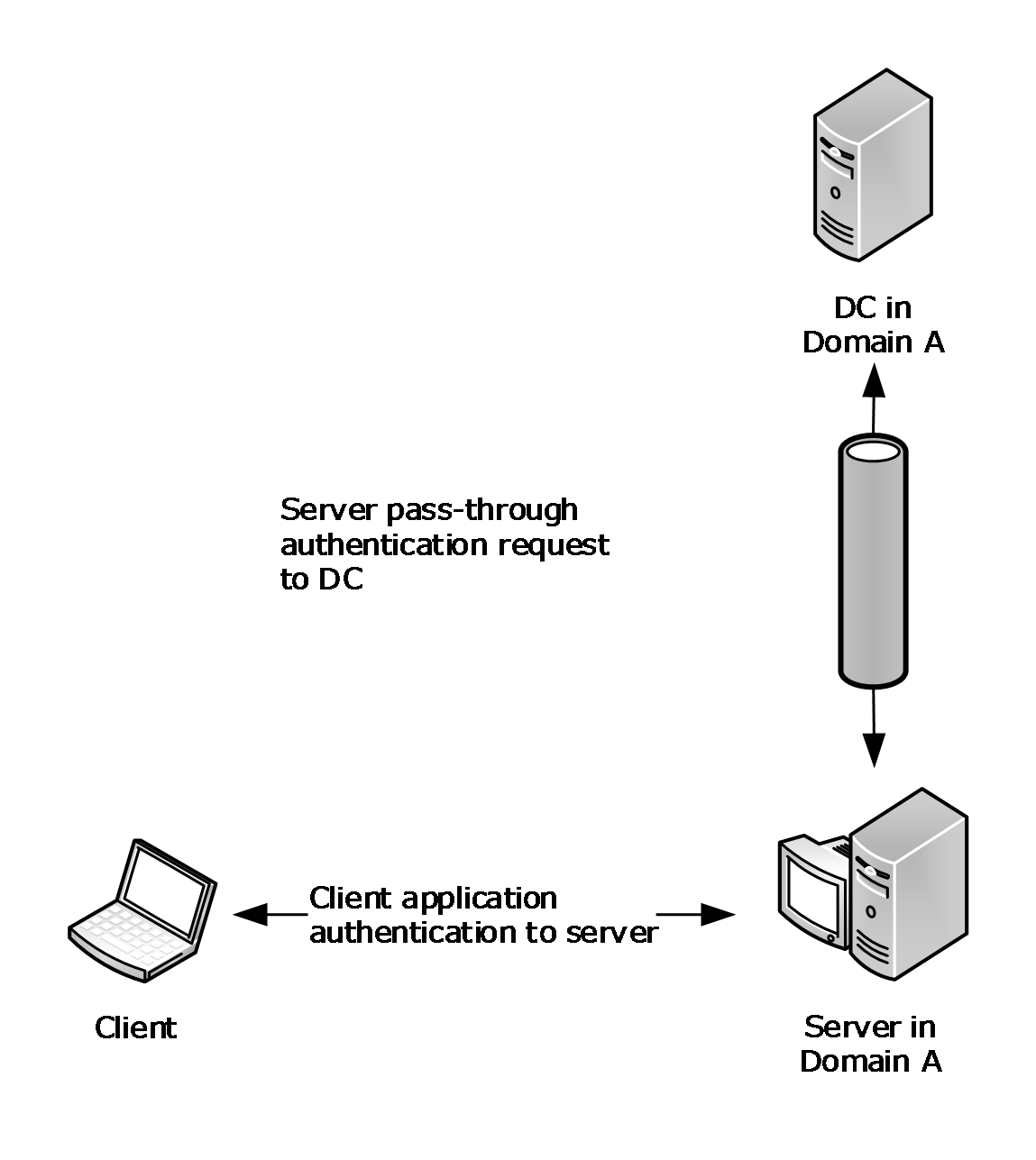


Figure 1: Pass-through authentication

### Pass-Through Authentication and Domain Trusts

The user account can be in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) other than the domain of the server. In that case, the [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) receiving the logon request from the server passes the request on to a DC in the domain of the user account. To make such scenarios work, the domain of the server (called the resource domain) and the domain of the user account (called the account domain) engage in a [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) relationship, in which authentication decisions made in the account domain are trusted in the resource domain. In such trust relationships, the resource domain is called the trusting domain, while the account domain is called the trusted domain. Trust relationships are established by administrators of the two domains.

The result of a trust establishment is a [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) (called a trust password) that DCs use in the two domains for computing the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) that is used for protecting the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) traffic. By using this secure channel, the DC in the resource domain can pass logon requests securely to the DC in the account domain, in the same way that the server passed the logon request to the former DC. The secure channel between DCs in two domains that are connected via a trust relationship is called a trusted domain secure channel. In contrast, the secure channel between the server and the DC in the resource domain is called a workstation secure channel. The following illustration depicts a process of pass-through authentication in which the authentication request is passed over two secure channels: from a server in Domain A to a DC in the same domain, and then from that DC to a DC in Domain B, which contains the user account.

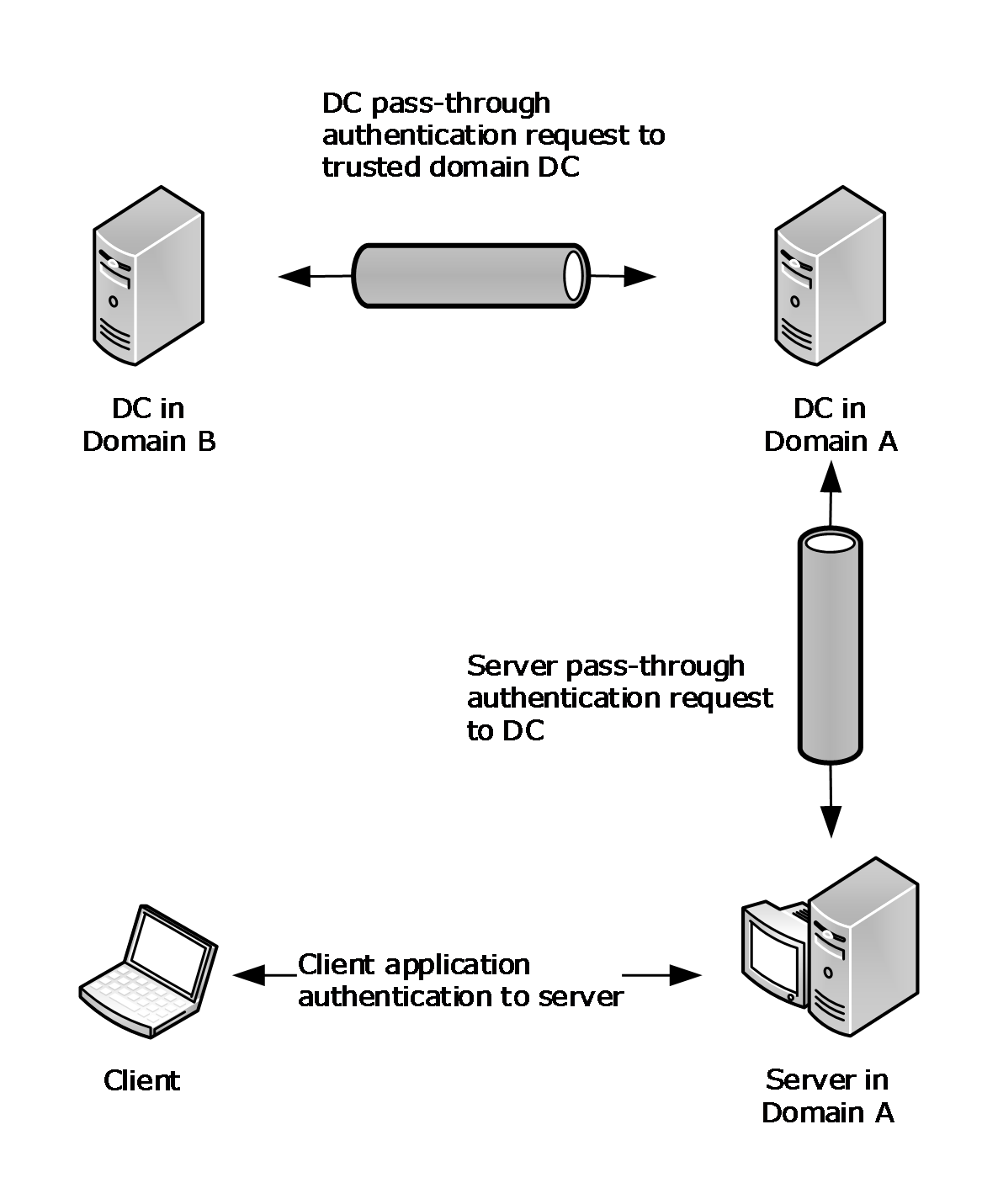


Figure 2: Pass-through authentication and domain trusts

In this scenario, the two domains are connected by means of a [**direct trust**](#gt_e03f25c6-dd6e-43df-83e2-98f89bcc50d9) relationship. Consider a scenario in which the two domains are connected by means of an "intermediate trust partner"; the resource domain trusts the intermediate domain, which in turn trusts the account domain. There can be multiple domains connected by means of trust relationships along the chain of direct domain trusts between the resource and the account domains. This type of trust relationship, in which the resource domain trusts the account domain through a chain of trust relationships between intermediate domains, is called [**transitive trust**](#gt_1c9fbb3f-ba87-419f-bd0c-39f73cee86f7). Each link in the transitive trust chain is backed by a shared secret used by DCs in two domains involved in the link for establishing the secure channel. Thus, the resource domain DC can deliver the logon request to the account domain DC over a chain of secure channels.

### Account Database Replication

Account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) replication is relevant only for server-to-server communication of the protocol.

So far we have considered scenarios in which there is one [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). In practice, multiple DCs are placed into a domain for redundancy and load balancing so that multiple DCs can service logon requests from many servers. In such scenarios, the DCs need to share the user account database.[<1>](#Appendix_A_1" \o "Product behavior note 1)[<2>](#Appendix_A_2" \o "Product behavior note 2)

A BDC was a domain controller that maintained a full copy of the [**domain account**](#gt_d0be6ce0-cc28-43cd-bd6b-6f324fcb8397) database and could satisfy authentication requests, but would not allow modification of the accounts. Instead, the BDCs of a domain replicate the account database from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) using account database replication methods.[<3>](#Appendix_A_3" \o "Product behavior note 3)[<4>](#Appendix_A_4" \o "Product behavior note 4)

To request and transfer the replication data securely, Netlogon uses the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) that the BDCs establish with the PDC by using the BDC's machine account password. This type of secure channel is called the server secure channel.

### Secure Channel Maintenance

The security of a channel based on a [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) depends on the secrecy of that shared value. Good cryptographic hygiene requires that such a shared value not be permanent. This protocol includes the facility to choose a new password and communicate it from the client to the [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). This allows client implementations of this protocol to set new passwords on machine accounts (if the request comes over a workstation [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca)) or on the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) accounts (if the request comes over a trusted [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) secure channel).

### Domain Trust Services

In some application scenarios, it can be desirable to obtain the list of [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6). For example, an application collecting user [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) might need to present the list of trusted domains from which users can choose their domains. The Netlogon Remote Protocol provides services to such applications via methods for retrieving domain trust information.

### Message Protection Services

Some applications might need to authenticate their messages sent to and received from a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). [**Windows Time Service (W32Time)**](#gt_43e51d0a-ac6a-4662-a99a-8f3029b78caf) is an example of such an application running on a machine that authenticates messages carrying time information received from the DC. The Netlogon Remote Protocol provides services to such applications via methods for computing a cryptographic digest of the message by using the machine account or [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password as the cryptographic key. By using these methods, the application running on the DC obtains the message digest and includes it in its response to the client. The application running on the client receives the message, obtains the message digest, and compares the digest with that received from the DC. If the two digests are the same, the client determines that the message was indeed sent by the DC.

### Administrative Services

Administrators might need to control or query the behavior related to Netlogon operations. For example, an administrator might want to force a change of the machine account password, or might want to reset the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to a particular [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). Netlogon provides such administrative services via methods for querying and controlling the server.

#### Netlogon Operational Flow on Domain Members

The first action that a Netlogon client performs on a [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) is finding a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in its [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) with which to set up the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca). This process is called the DC discovery. After a DC is discovered, the domain member sets up a secure channel to the DC.

For all subsequent requests from the client to the DC pertaining to authentication, the Netlogon Remote Protocol transmits the request by using the secure channel. The Netlogon Remote Protocol receives the user validation data over the secure channel from the DC and returns the data to the authentication protocol.

Periodically, the operating system can use the Netlogon Remote Protocol to change the machine account password.

#### Netlogon Operational Flow on Domain Controllers

Upon receiving a logon request, Netlogon determines the account [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) of the user being authenticated. Netlogon determines the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) link over which to send the request toward the account domain. Netlogon finds a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the trusted domain on that link and sets up the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to that DC by using the trust password for the trusted domain. Netlogon passes the logon request through to that DC. Netlogon receives the user validation data from that DC and returns the data to the secure channel client making the logon request.

Netlogon synchronizes BDC account [**databases**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) with the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) account database.

Periodically, Netlogon changes the machine account password for the DC. On the PDC, Netlogon periodically changes trust passwords for all directly trusted domains.

Netlogon performs the aforementioned services requested by applications or administrators.

### Netlogon Structures and Methods

The Netlogon Remote Protocol structures and methods that are specified in section [2.2.1](#Section_c3a0defffd1b4df9850f420cb8a224f5) and section [3.5.4](#Section_256678803d51499bb22819c08eb16b81) are grouped according to the Netlogon scenarios and operational flows as follows:

* [DC Location Structures (section 2.2.1.2)](#Section_94c3b27ad8064eacbfe15a48e63eeca9) and [DC Location Methods (section 3.5.4.3)](#Section_2c26616cfe894d0288aea56356e0f512). This protocol uses the structures and methods in this group to locate a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd)in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). Methods in this group are also used for obtaining the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) information that is related to DC discovery, as well as for maintaining [**Domain Name System (DNS)**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) registration information for DCs.
* [Secure Channel Establishment and Maintenance Structures (section 2.2.1.3)](#Section_fb50db727f71478da18012eb0ca3b36b) and [Secure Channel Establishment and Maintenance Methods (section 3.5.4.4)](#Section_641f684e080943f38ba92a3754874126). Structures and methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used for setting up and maintaining the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca).
* [Pass-Through Authentication Structures (section 2.2.1.4)](#Section_d76f87d0b8a142e8b3b147ab47444cbc) and [Pass-Through Authentication Methods (section 3.5.4.5)](#Section_24933c92b96540f19e1d74ea27d4813c). These structures and methods are used for performing pass-through authentication and obtaining user validation information.
* [Account Database Replication Structures (section 2.2.1.5)](#Section_c4adbfb3678b4996860f3602709558b9) and [Account Database Replication Methods (section 3.5.4.6)](#Section_5657e68eab5b4d9998b80fcaa1bdffc6). These structures and methods were used in the account database replication.
* [Domain Trust Structures (section 2.2.1.6)](#Section_26bc3213bff74ed5ac5b651bab12d874) and [Domain Trust Methods (section 3.5.4.7)](#Section_d6ee9b3a1cf24719a82773f2e0298336). Structures and methods in this group are used for retrieving domain [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) information.
* [Message Protection Methods (section 3.5.4.8)](#Section_fff9e47b029f41e0b48b1f5c5554b68f). Methods in this group are used for performing the message protection services.
* [Administrative Services Structures (section 2.2.1.7)](#Section_3b7ad20ab8c64191971e8b96f85d0899) and [Administrative Services Methods (section 3.5.4.9)](#Section_647e0ebb338f499fabbc8f82adcb36ff). This group of structures and methods is used for querying and controlling the Netlogon Remote Protocol server.
* [Obsolete Structures (section 2.2.1.8)](#Section_7a86a6835c4a4a71b0659c73f6c1beb8) and [Obsolete Methods (section 3.5.4.10)](#Section_a9dccfcfea6e4f919c0739183708e34e). The structures and methods in this group are unsupported and obsolete.

#### History of Netlogon

The Netlogon Remote Protocol is an older protocol that predates Windows NT and has been through multiple revisions and expansions. As a result, some of the methods are not used in non–LAN Manager environments, and new structures and methods were introduced to support the new functionality required.[<5>](#Appendix_A_5" \o "Product behavior note 5)

##### New Methods Derived from Existing Methods

In many cases, a new method would differ from an existing method by the addition of one or a few new parameters. In such cases, one of two naming conventions was used. One convention was that the new method would typically be named identically to the existing method, except for the addition of a suffix such as Ex (to mean Extended, as in the [DsrGetDcNameEx](#Section_5de19b7e4ce34cc4978f8959f46797ba) method, which is the extended version of the original [DsrGetDcName](#Section_86a3fa5b1f0e412a942f33a10e5e9eff) method). The other convention was to add a numeral value to reflect the method revision number (as in the [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355) method and [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) method, which are the new versions of the original [NetrServerAuthenticate](#Section_2561f16011f943a7bad45721a05e8ad8) method).

##### Using Dummy Fields in Structures

The requirements of this protocol have evolved over time. During the original design phase, typed but unused fields were appended to some structures. In later versions of the protocol, if new data needed to be transmitted between the client and the server, these fields could be used without ill effects, so long as the type of the data was preserved. The servers of a previous version of the Netlogon protocol would receive and ignore the fields.

In many cases, an introduction of a new Ex structure necessitated an introduction of a corresponding Ex [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) method for passing the new structure between the client and the server. As an alternative to the growing number of Ex structures and methods, an approach was introduced to avoid the addition of new structures and methods by using dummy fields. New structures would have a few unused fields, such as **DummyString1**, **DummyString2**, **DummyLong1**, and **DummyLong2**. These dummy fields allow additional information that was not conceived originally to be passed through the interface in a safe fashion. If the structure has not been extended, these fields are set to zero and ignored upon receipt.

For example, a dummy field **DummyString1** of the [NETLOGON\_ONE\_DOMAIN\_INFO (section 2.2.1.3.10)](#Section_77cd977686124dab9748bfb07247fd4c) structure was used at one point to carry [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) extension attributes. As a dummy field got used, it might or might not be renamed. In the case of NETLOGON\_ONE\_DOMAIN\_INFO, **DummyString1** was renamed as **TrustExtension** to reflect the new nature of the field. This scheme of dummy field usage worked well: this protocol running on a new client receiving the NETLOGON\_ONE\_DOMAIN\_INFO structure would use the **TrustExtension** field as appropriate, while the NETLOGON\_ONE\_DOMAIN\_INFO running on an old client would completely ignore the **DummyString1** field.

##### Fields and Structures Used by Netlogon Pass-through Methods

During the design of the **NetrLogonSamLogon** method which is used for Netlogon pass-through, three fields were created to pass information opaquely for applications:

* **LogonLevel**
* **LogonInformation**
* **ValidationLevel**

At that time, it was thought that there would be four types of logon:

* Interactive
* Network
* Service
* Generic

However, only three were used: Interactive, Network, and Generic. Service type remains an option that can be used by callers, and like all Netlogon pass-through behavior, it is specified by the receiving protocol.

##### Using Negotiated Flags

The client and the server often need to know the capabilities of their partners in their client/server communications. For example, it is sometimes necessary or desirable for a newer version client to avoid calling a method that the older version server does not implement. Similarly, the new server would avoid sending fields that the older client is going to treat as dummies and ignore. To make this possible, the client and the server need to establish a common set of capabilities that both the client and the server support.

For this reason, the [NetrServerAuthenticate3 (section 3.5.4.4.2)](#Section_3a9ed16f801445ae80afc0ecb06e2db9) method, which is called early on during setup of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) between the client and the server, includes the *NegotiateFlags* parameter. The *NegotiateFlags* parameter uses a set of bit flags to carry the client and server capabilities. The client sets its capabilities on input, and the server responds with capabilities that it supports out of those sent by the client. The resulting set of bit flags is the set of capabilities that the client and the server mutually support.

## Relationship to Other Protocols

The Netlogon Remote Protocol depends on [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) and on the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) datagram delivery service, as specified in [[MS-SMB]](%5bMS-SMB%5d.pdf#Section_f210069c70864dc2885e861d837df688), which are its transports.

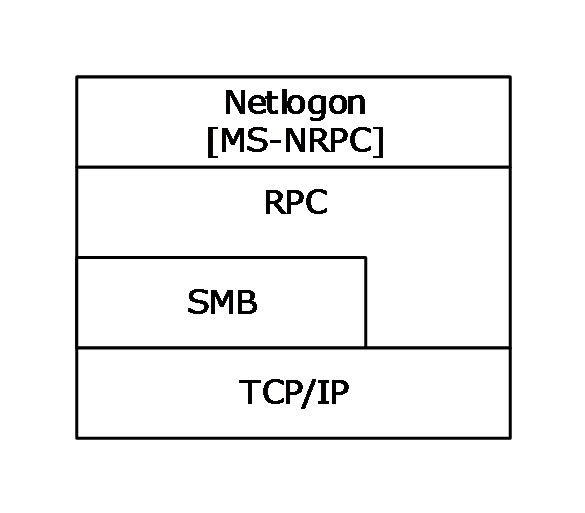


Figure 3: Transport relationships

Other non-RFC standard specifications relevant to the implementation of the Netlogon Remote Protocol are:

* Directory Technical Specification [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) defines Active Directory data types, data structures, and their interactions, many of which are relevant to the functioning of the Netlogon Remote Protocol.
* Group Policy: Security Protocol Extension [[MS-GPSB]](%5bMS-GPSB%5d.pdf#Section_6a07a06be62847659d910d63ba47fdc0) is for managing [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) signing and encryption settings.
* Local Security Authority (Domain Policy) Remote Protocol Specification [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) is used for accessing certain directory information.
* NT LAN Manager (NTLM) Authentication Protocol Specification [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) uses netlogon for pass-through authentication and specifies how to do one-way functions (OWF) of the computer password.
* Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server) [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) is used for account lookup during session-key negotiation.

Authentication Protocol Domain Support Specification [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) is an example of how authentication protocols can use generic pass-through (section [3.2.4.1](#Section_fe2775d4a3e24971a2558eef8dd27a27)).

## Prerequisites/Preconditions

This protocol is an [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) interface and, as a result, has the prerequisites that [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) specifies as being common to RPC interfaces.

Netlogon replication uses the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) datagram delivery mechanism; therefore, it depends on this mailslot delivery mechanism being operational before Netlogon begins operation. For mailslot operational requirements, see [[MS-MAIL]](%5bMS-MAIL%5d.pdf#Section_8ea19aa46e5a4aedb6280b5cd75a1ab9) section 1.5. For more information about the mailslot delivery mechanism, see [[MS-CIFS]](%5bMS-CIFS%5d.pdf#Section_d416ff7cc536406ea9514f04b2fd1d2b) section 2.2.4.33.

To use this protocol or to use Netlogon as a [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a), a computer requires a [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) (section [3.1.1](#Section_708b71329e72447c992bd0bef4078f81)) with the [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

The client of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is required to discover the DC to which it is establishing a secure channel. Thus, a [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) discovers a DC in its [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

A BDC discovers the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) in its domain. A DC discovers a DC for each of its [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domains.

Upon establishing a secure channel, a client can call any of the methods of this protocol that require a secure channel. This requires both the client and the server to have a working RPC implementation, including the security extensions ([MS-RPCE] section 2.2.1.1.7). For a complete list of methods that require a secure channel, see section [3.5](#Section_1b79123d2f1e4970b9e8ea74ba95f95a).

All methods of this protocol are RPC calls from the client to the server that perform the complete operation in a single call. No shared state between the client and server is assumed other than the [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) that was previously established. There are no restrictions on the number of times that a method can be called or the order in which methods can be called, unless explicitly noted in sections [3.4](#Section_2e745bde2f654857bd3c7de7b191c35a) and 3.5.

The Netlogon Remote Protocol client and server can run only on domain-joined systems. This protocol is enabled or disabled during the domain join and unjoin tasks as described in [[MS-ADOD]](%5bMS-ADOD%5d.pdf#Section_5ff67bf4c14548cb89cd4f5482d94664) and specified in [[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) sections 3.2.4.12, 3.2.4.13, and 3.2.4.14.

## Applicability Statement

The Netlogon Remote Protocol contains an implementation of a [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a), which provides packet encryption and signing services to secure client and server communication at the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) packet level. These security services SHOULD[<6>](#Appendix_A_6" \o "Product behavior note 6) be used for establishing a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) for RPC-based client-to-server communication.

The Netlogon Remote Protocol can act as a secure transport for NTLM authentication and for other authentication mechanisms between arbitrary servers and the account authority or [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) for that server. The Netlogon Remote Protocol also provides methods for maintaining the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password for all trusted domains. Additional information for the methods in this topic is provided in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413) for cases where the server is not a member of a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) and resolves requests independently.

## Versioning and Capability Negotiation

* Supported Transports: This protocol uses the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) datagram delivery service, [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) over named pipes ([[PIPE]](https://go.microsoft.com/fwlink/?LinkId=90247)), and RPC over TCP/IP as its only transports. Also see section [2.1](#Section_592edbc8f6f140c09ab3fe6725ac6d7e).
* Security and Authentication Methods: As specified in section [3.2](#Section_8ea3ca7111074888b108f5bdcb350eea) and [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 1.7.
* Protocol Version: This protocol's RPC interface has a single version number of 1.0. Microsoft can extend this protocol by adding RPC methods to the interface with [**opnums**](#gt_e127848e-c66d-427d-b3aa-9f904fa4ada7) lying numerically beyond those defined in this document. A client determines whether such methods are supported by attempting to invoke the method. If the version of the interface does not implement the method being invoked, it is required that the RPC server return an opnum out of range error. RPC versioning and capability negotiation for this situation is specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) and [MS-RPCE] section 2.1.

For methods with multiple definitions (for example, [NetrServerAuthenticate (section 3.5.4.4.4)](#Section_2561f16011f943a7bad45721a05e8ad8), [NetrServerAuthenticate2 (section 3.5.4.4.3)](#Section_985982ae9aa84565b30b33d6353d3355), and [NetrServerAuthenticate3 (section 3.5.4.4.2)](#Section_3a9ed16f801445ae80afc0ecb06e2db9)), the Netlogon Remote Protocol first tries the most recent definition of the method for which it has code. If that fails, this protocol tries the next most recent definition, and so on. Using the NetrServerAuthenticate example, this protocol tries NetrServerAuthenticate3 first, NetrServerAuthenticate2 second, and finally NetrServerAuthenticate.

* Capability Negotiation: When a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is established, the *NegotiateFlags* parameter of the NetrServerAuthenticate2 and NetrServerAuthenticate3 methods is used to negotiate a common set of capabilities that each of the participants in the negotiation can support. See section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed).

## Vendor-Extensible Fields

This protocol uses NTSTATUS values as defined in [[MS-ERREF]](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90) section 2.3. Vendors are free to choose their own values for this field, as long as the C bit (0x20000000) is set, indicating it is a customer code.

## Standards Assignments

This protocol uses the following [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) [**UUID**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3), [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee), and [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) assignments:

| Parameter | Value | Reference |
| --- | --- | --- |
| RPC interface UUID | 12345678-1234-ABCD-EF00-01234567CFFB | Section [2.1](#Section_592edbc8f6f140c09ab3fe6725ac6d7e) |
| Pipe name | \PIPE\NETLOGON | Section 2.1 |
| Mailslot name | \MAILSLOT\NET\NETLOGON | Section 2.1 |

# Messages

## Transport

This protocol uses the following [**RPC protocol sequences**](#gt_0c171cc7-e9c4-41b6-95a9-536db0042c7a) as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.1:

* [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) over TCP/IP
* RPC over named pipes

This protocol uses RPC [**dynamic endpoints**](#gt_46da887f-3f66-4941-a854-e51c52cf4c56) for RPC over TCP/IP, as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 4.

This protocol uses the following well-known [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee). This endpoint is a named pipe for RPC over SMB:

* \PIPE\NETLOGON

This protocol uses the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) datagram delivery service ([[MS-MAIL]](%5bMS-MAIL%5d.pdf#Section_8ea19aa46e5a4aedb6280b5cd75a1ab9) and [[MS-SMB]](%5bMS-SMB%5d.pdf#Section_f210069c70864dc2885e861d837df688)). Mailslot messages (see [MS-MAIL] section 2.2.1) are sent to the following mailslot:

* \MAILSLOT\NET\NETLOGON. This named mailslot is used in Netlogon replication, as defined in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

This protocol MUST use the [**universally unique identifier (UUID)**](#gt_c4813fc3-b2e5-4aa3-bde7-421d950d68d3) 12345678-1234-ABCD-EF00-01234567CFFB. The RPC version number is 1.0.

This protocol uses the Netlogon SSP. The server MUST use the RPC [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) extensions ([MS-RPCE] section 2.2.1.1.7). It MUST register the Netlogon security package as specified in section [3.3](#Section_388e4b68f4e44e0498ecdfae7e9b1f01).

## Common Data Types

In addition to the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) base types and definitions that are specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 4.2.9 and [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2, additional data types are defined in the following sections.

### Structures and Enumerated Types

This section specifies structures and enumerated types that are used by the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) methods specified in section [3.5](#Section_1b79123d2f1e4970b9e8ea74ba95f95a). Section [2.2.1.1](#Section_5fc4156477124f478ca634edc1721bae) specifies the basic structures that are elementary to this protocol and which are used by many methods. In the sections that follow 2.2.1.1, structures are grouped according to their usage scenarios as described in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

#### Basic Structures

The structures in this group do not fall into any particular category of Netlogon usage scenarios. They are used by multiple Netlogon Remote Protocol methods.

##### CYPHER\_BLOCK

The CYPHER\_BLOCK structure defines an encrypted eight-character string. The type of encryption used is application-dependent.

1. typedef struct \_CYPHER\_BLOCK {
2. CHAR data[8];
3. } CYPHER\_BLOCK,
4. \*PCYPHER\_BLOCK;

**data:**  An encrypted eight-character string.

##### STRING

The STRING structure contains the length, the maximum length, and a pointer to a buffer containing the string.

1. typedef struct \_STRING {
2. USHORT Length;
3. USHORT MaximumLength;
4. [size\_is(MaximumLength), length\_is(Length)]
5. CHAR \* Buffer;
6. } STRING,
7. \*PSTRING;

**Length:**  The length of the data pointed to by **Buffer**, in bytes.

**MaximumLength:**  The total allocated length of the data pointed to by **Buffer**, in bytes.[<7>](#Appendix_A_7" \o "Product behavior note 7)

**Buffer:**  A pointer to a buffer containing the character string.

##### LM\_OWF\_PASSWORD

The LM\_OWF\_PASSWORD structure carries a [**one-way function (OWF)**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of a LAN Manager password. The LM\_OWF\_PASSWORD structure MAY be encrypted, as specified by each method that uses this structure. See the [NetrServerPasswordSet](#Section_a93310347f3047bd8aee93bbabe90df4) method in section 3.5.4.4.6 for encryption information.

1. typedef struct \_LM\_OWF\_PASSWORD {
2. CYPHER\_BLOCK data[2];
3. } LM\_OWF\_PASSWORD,
4. \*PLM\_OWF\_PASSWORD,
5. ENCRYPTED\_LM\_OWF\_PASSWORD,
6. \*PENCRYPTED\_LM\_OWF\_PASSWORD;

**data:**  An array of [CYPHER\_BLOCK (section 2.2.1.1.1)](#Section_56a8d298dbeb4eb5ad9876536ec352f8) data structures that contains the LMOWFv1 of a password. LMOWFv1 is specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1.

##### NT\_OWF\_PASSWORD

The NT\_OWF\_PASSWORD structure defines a [**one-way function (OWF)**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of a Windows NT operating system [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) password. The NT\_OWF\_PASSWORD structure can be encrypted, as specified by each method that uses this structure. When this structure is encrypted, Netlogon methods can use the DES encryption algorithm in ECB mode, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.11.1.1 Encrypting an NT Hash or LM Hash Value with a specified key. The [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is the specified 16-byte key used to derive its keys using the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4. For specific encryption information, see the individual methods, such as [NetrServerTrustPasswordsGet (section 3.5.4.4.8)](#Section_84b0d22a9b2c44328ae04a72eda28ea4) and [NetrServerGetTrustInfo (section 3.5.4.7.6)](#Section_4c2296c3c6f047fc9f01a6fe17bf1d5b).

1. typedef struct \_NT\_OWF\_PASSWORD {
2. CYPHER\_BLOCK data[2];
3. } NT\_OWF\_PASSWORD,
4. \*PNT\_OWF\_PASSWORD,
5. ENCRYPTED\_NT\_OWF\_PASSWORD,
6. \*PENCRYPTED\_NT\_OWF\_PASSWORD;

**data:**  An array of [CYPHER\_BLOCK (section 2.2.1.1.1)](#Section_56a8d298dbeb4eb5ad9876536ec352f8) structures that contains the NTOWFv1 of a password. NTOWFv1 is specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1.

##### NETLOGON\_AUTHENTICATOR

The NETLOGON\_AUTHENTICATOR structure defines an authentication [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8).

1. typedef struct \_NETLOGON\_AUTHENTICATOR {
2. NETLOGON\_CREDENTIAL Credential;
3. DWORD Timestamp;
4. } NETLOGON\_AUTHENTICATOR,
5. \*PNETLOGON\_AUTHENTICATOR;

**Credential:**  A [NETLOGON\_CREDENTIAL (section 2.2.1.3.4)](#Section_d55e263271634f6cb6624b870e8cc1cd) structure that contains the encrypted portion of the [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**Timestamp:**  An integer value that contains the time of day at which the client constructed this authentication credential, represented as the number of elapsed seconds since 00:00:00 of January 1, 1970. The authenticator is constructed just before making a call to a method that requires its usage.

#### DC Location Structures

The structures in this group relate to locating a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### DOMAIN\_CONTROLLER\_INFOW

The DOMAIN\_CONTROLLER\_INFOW structure SHOULD[<8>](#Appendix_A_8" \o "Product behavior note 8) define information returned by the following methods: [DsrGetDcName (section 3.5.4.3.3)](#Section_86a3fa5b1f0e412a942f33a10e5e9eff), [DsrGetDcNameEx (section 3.5.4.3.2)](#Section_5de19b7e4ce34cc4978f8959f46797ba), and [DsrGetDcNameEx2 (section 3.5.4.3.1)](#Section_fb8e1146a0454c3198d1c68507ad5620). This structure is used to describe naming and addressing information about a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

1. typedef struct \_DOMAIN\_CONTROLLER\_INFOW {
2. [string, unique] wchar\_t\* DomainControllerName;
3. [string, unique] wchar\_t\* DomainControllerAddress;
4. ULONG DomainControllerAddressType;
5. GUID DomainGuid;
6. [string, unique] wchar\_t\* DomainName;
7. [string, unique] wchar\_t\* DnsForestName;
8. ULONG Flags;
9. [string, unique] wchar\_t\* DcSiteName;
10. [string, unique] wchar\_t\* ClientSiteName;
11. } DOMAIN\_CONTROLLER\_INFOW,
12. \*PDOMAIN\_CONTROLLER\_INFOW;

**DomainControllerName:**  A pointer to a null-terminated UTF-16 string that contains a NetBIOS or [**fully qualified domain name (FQDN) (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) of the DC, prefixed with "\\".

**DomainControllerAddress:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the DC address, prefixed with "\\". The string can be either a textual representation of an IPv4/IPv6 address[<9>](#Appendix_A_9" \o "Product behavior note 9) or the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the DC, determined by the **DomainControllerAddressType** field.

**DomainControllerAddressType:**  A 32-bit value indicating the DC address type, which MUST be one, and only one, of the following.

| Value | Meaning |
| --- | --- |
| 0x00000001 | The address is a string that contains an IPv4 address in dotted-decimal notation (for example, 192.168.0.1), or an IPv6 address in colon-separated notation.[<10>](#Appendix_A_10" \o "Product behavior note 10) |
| 0x00000002 | The address is a NetBIOS name. |

**DomainGuid:**  A [**globally unique identifier (GUID)**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) structure ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.4.1) that contains an identifier for the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). When there is no domain GUID, this field MUST be set to zero.[<11>](#Appendix_A_11" \o "Product behavior note 11) A GUID can be used across all computers and networks wherever a unique identifier is required.

**DomainName:**  A pointer to a Unicode string that contains the NetBIOS or FQDN (1) of the domain.

**DnsForestName:**  A pointer to a null-terminated Unicode string that contains the FQDN (1) of the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62).

**Flags:**  A set of bit flags in little-endian format that describe the features and roles of the DC. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table, with the exceptions that bit J cannot be combined with A, B, D, E, or P; bit F cannot be combined with I; and bit K cannot be combined with L.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| O | N | M | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | S | R | Q | P | L | K | J | I | H | G | F | E | D | C | B | 0 | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | The DC is the domain's [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). |
| B | The DC contains the [**global catalog (GC)**](#gt_4f5d605a-7b3f-4db7-8c21-b146856d7169) for the forest [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90). |
| C | The DC supports the Lightweight Directory Access Protocol (LDAP). |
| D | The DC supports a [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e). |
| E | The DC is a Kerberos [**Key Distribution Center (KDC)**](#gt_6e5aafba-6b66-4fdd-872e-844f142af287). |
| F | The DC has a network time service available but no clock hardware. |
| G | The DC is in the closest [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) to the client. |
| H | The DC has a writable directory service available. |
| I | The DC has clock hardware and a network time service available. |
| J | The DC is an LDAP server servicing an Application [**naming context (NC)**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.1.5). |
| K | The DC is a [**read-only domain controller (RODC)**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870).[<12>](#Appendix_A_12" \o "Product behavior note 12) |
| L | The server is a [**writable domain controller**](#gt_9d964ddb-09d6-4a1b-b27b-42adabc07993).[<13>](#Appendix_A_13" \o "Product behavior note 13) |
| M | The DC's name is a [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) name. |
| N | The DC's [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) is a DNS name. |
| O | The DC's forest name is a DNS name. |
| P | The DC has an Active Directory Web Service available.[<14>](#Appendix_A_14" \o "Product behavior note 14) |
| Q | The DC has a functional level of DS\_BEHAVIOR\_WIN2012 or later. |
| R | The DC has a functional level of DS\_BEHAVIOR\_WIN2012R2 or later. |
| S | The DC has a functional level of DS\_BEHAVIOR\_WIN2016 or later. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**DcSiteName:** A pointer to a null-terminated Unicode string that SHOULD[<15>](#Appendix_A_15" \o "Product behavior note 15) contain the site name that is associated with the DC. When there is no associated site, this field MUST be NULL.

**ClientSiteName:**  A pointer to a null-terminated Unicode string that contains the client's site name. When there is no client site name, this field MUST be NULL.

##### NL\_SITE\_NAME\_ARRAY

The NL\_SITE\_NAME\_ARRAY structure defines an array of [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) names.

1. typedef struct \_NL\_SITE\_NAME\_ARRAY {
2. ULONG EntryCount;
3. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SiteNames;
4. } NL\_SITE\_NAME\_ARRAY,
5. \*PNL\_SITE\_NAME\_ARRAY;

**EntryCount:**  The number of entries in **SiteNames**.

**SiteNames:**  A pointer to an array of null-terminated RPC\_UNICODE\_STRING strings ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10) that contain site names. For more information about sites, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.1.2.2.1.

##### NL\_SITE\_NAME\_EX\_ARRAY

The NL\_SITE\_NAME\_EX\_ARRAY structure defines an array of [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) and subnet names. This structure extends the [NL\_SITE\_NAME\_ARRAY (section 2.2.1.2.2)](#Section_4c5fb44a6d68420d970e68ad5436bbd3) structure by adding an array of subnets that correspond to the sites.

1. typedef struct \_NL\_SITE\_NAME\_EX\_ARRAY {
2. ULONG EntryCount;
3. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SiteNames;
4. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SubnetNames;
5. } NL\_SITE\_NAME\_EX\_ARRAY,
6. \*PNL\_SITE\_NAME\_EX\_ARRAY;

**EntryCount:**  The number of entries in **SiteNames** and **SubnetNames**.

**SiteNames:**  A pointer to an array of null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) strings that contain site names. For details about sites, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.1.2.2.1.

**SubnetNames:**  A pointer to an array of null-terminated Unicode strings that contain subnet names. For details about subnets, see [MS-ADTS] section 6.1.1.2.2.2.1.

##### NL\_SOCKET\_ADDRESS

The NL\_SOCKET\_ADDRESS structure contains a socket address.

1. typedef struct \_NL\_SOCKET\_ADDRESS {
2. [size\_is(iSockaddrLength)] UCHAR \* lpSockaddr;
3. ULONG iSockaddrLength;
4. } NL\_SOCKET\_ADDRESS,
5. \*PNL\_SOCKET\_ADDRESS;

**lpSockaddr:**  A pointer to an octet string. The format of the **lpSockaddr** member when an IPv4 socket address is used is specified in section [2.2.1.2.4.1](#Section_75981bfba7bb41bc8705388531af6ed8). The format of the **lpSockaddr** member when an IPv6 socket address is used is specified in section [2.2.1.2.4.2](#Section_f8e21b2b6ea54eb9a350acdabe33cc93).

**iSockaddrLength:**  The length of the octet string pointed to by **lpSockaddr**, in bytes.

###### IPv4 Address Structure

The IPv4\_Sockaddr structure specifies the format of an IPv4 socket address. This structure is built as if on a little-endian machine, and is treated as a byte array.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| AddressFamily | | | | | | | | | | | | | | | | Port | | | | | | | | | | | | | | | |
| Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Padding | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**AddressFamily (2 bytes):** The address family; MUST be 0x0002.

**Port (2 bytes):** An IP port number.

**Address (4 bytes):** An IP address, as specified in [[RFC791]](https://go.microsoft.com/fwlink/?LinkId=392659).

**Padding (8 bytes):** Set to zero. This field is ignored by the server.

###### IPv6 Address Structure

The IPv6\_Sockaddr structure specifies the format of an IPv6 socket address. This structure is built as if on a little-endian machine, and is treated as a byte array.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| AddressFamily | | | | | | | | | | | | | | | | Port | | | | | | | | | | | | | | | |
| FlowInfo | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Address (16 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ScopeID | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**AddressFamily (2 bytes):** Address family; MUST be 0x0017.

**Port (2 bytes):** An IP port number.

**FlowInfo (4 bytes):** Flow information. This field is not currently used by the protocol. The field MUST be set to zero and MUST be ignored on receipt.

**Address (16 bytes):** An IP address, as specified in [[RFC3493]](https://go.microsoft.com/fwlink/?LinkId=90425).

**ScopeID (4 bytes):**  Set of interfaces for a scope, as specified in [RFC3493].

##### NL\_DNS\_NAME\_INFO

The NL\_DNS\_NAME\_INFO structure provides the information on a [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) name (record) (as specified in [[RFC2782]](https://go.microsoft.com/fwlink/?LinkId=90381)) to be updated by the [DsrUpdateReadOnlyServerDnsRecords (section 3.5.4.3.11)](#Section_e83df1615c134520ae5a79218ed0bb19) method. The DsrUpdateReadOnlyServerDnsRecords method will update DNS as requested by the **Register** field's value in this structure.

1. typedef struct \_NL\_DNS\_NAME\_INFO {
2. ULONG Type;
3. [string] wchar\_t\* DnsDomainInfo;
4. ULONG DnsDomainInfoType;
5. ULONG Priority;
6. ULONG Weight;
7. ULONG Port;
8. UCHAR Register;
9. ULONG Status;
10. } NL\_DNS\_NAME\_INFO,
11. \*PNL\_DNS\_NAME\_INFO;

**Type:**  The type of DNS name, which MUST be one, and only one, of the following:

| Value | Meaning |
| --- | --- |
| NlDnsLdapAtSite  22 | \_ldap.\_tcp.<SiteName>.\_sites.<DnsDomainName>.  Allows a client to find an LDAP server in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) named by <DnsDomainName>, and is in the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) named by <SiteName>. |
| NlDnsGcAtSite  25 | \_ldap.\_tcp.<SiteName>.\_sites.gc.\_msdcs.<DnsForestName>.  Allows a client to find a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) serving a [**global catalog (GC)**](#gt_4f5d605a-7b3f-4db7-8c21-b146856d7169) in the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) named by <DnsForestName>, and is in the site named by <SiteName>. |
| NlDnsDsaCname  28 | <DsaGuid>.\_msdcs.<DnsForestName>.  Allows a client to find a DC in the forest named by <DnsForestName> based on the DSA [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). For a definition of DSA GUID, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 1.1. |
| NlDnsKdcAtSite  30 | \_kerberos.\_tcp.<SiteName>.\_sites.dc.\_msdcs.<DnsDomainName>.  Allows a client to find a DC running a Kerberos [**KDC**](#gt_6e5aafba-6b66-4fdd-872e-844f142af287) in the domain named by <DnsDomainName>, and is in the site named by <SiteName>. |
| NlDnsDcAtSite  32 | \_ldap.\_tcp.<SiteName>.\_sites.dc.\_msdcs.<DnsDomainName>.  Allows a client to find a DC in the domain named by <DnsDomainName>, and is in the site named by <SiteName>. |
| NlDnsRfc1510KdcAtSite  34 | \_kerberos.\_tcp.<SiteName>.\_sites.<DnsDomainName>.  Allows a client to find a RFC-1510 compliant Kerberos KDC in the domain named by <DnsDomainName>, and is in the site named by <SiteName>. |
| NlDnsGenericGcAtSite  36 | \_gc.\_tcp.<SiteName>.\_sites.<DnsForestName>.  Allows a client to find a global catalog (GC) server in the forest named by <DnsForestName>, and is in the site named by <SiteName>. |

**DnsDomainInfo:**  The string that will be based on the **DnsDomainInfoType** defined below.

**DnsDomainInfoType:**  The type of **DnsDomainInfo** member, which MUST be one, and only one, of the following.

| Value | Meaning |
| --- | --- |
| NlDnsDomainName  1 | The **DnsDomainInfo** member is a DNS [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c). |
| NlDnsDomainNameAlias  2 | The **DnsDomainInfo** member is a DNS domain name [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd). |
| NlDnsForestName  3 | The **DnsDomainInfo** member is a DNS forest name. |
| NlDnsForestNameAlias  4 | The **DnsDomainInfo** member is a DNS forest name alias. |
| NlDnsNdncDomainName  5 | The **DnsDomainInfo** member is a non-domain [**NC**](#gt_784c7cce-f782-48d8-9444-c9030ba86942) (application NC) name. For a definition of application NC, see [MS-ADTS] section 1.1. |
| NlDnsRecordName  6 | The **DnsDomainInfo** member is a DNS record name that is required to be deregistered. This is valid only for deregistration in which the Register value is set to FALSE. For the types of DNS record name, see [MS-ADTS] section 6.3.2. |

**Priority:** The priority for DNS SRV records.

**Weight:** The weight for DNS SRV records.

**Port:** The port for the DNS SRV record.

**Register:** Zero indicates to deregister the DNS name; other values indicate to register the DNS name.

**Status:** The update status of the DNS name. Status SHOULD[<16>](#Appendix_A_16" \o "Product behavior note 16) be set to 0x00000000 on success; otherwise, it contains a nonzero error code.

##### NL\_DNS\_NAME\_INFO\_ARRAY

The NL\_DNS\_NAME\_INFO\_ARRAY structure provides the information on [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) names (records) to be updated by the [DsrUpdateReadOnlyServerDnsRecords (section 3.5.4.3.11)](#Section_e83df1615c134520ae5a79218ed0bb19) method.

1. typedef struct \_NL\_DNS\_NAME\_INFO\_ARRAY {
2. ULONG EntryCount;
3. [size\_is(EntryCount)] PNL\_DNS\_NAME\_INFO DnsNamesInfo;
4. } NL\_DNS\_NAME\_INFO\_ARRAY,
5. \*PNL\_DNS\_NAME\_INFO\_ARRAY;

**EntryCount:** The number of entries in the **DnsNamesInfo** field.

**DnsNamesInfo:** A pointer to an array of the [NL\_DNS\_NAME\_INFO (section 2.2.1.2.5)](#Section_1c7e652045a243e1ac0b43e771f85b14) structure, which SHOULD[<17>](#Appendix_A_17" \o "Product behavior note 17) contain DNS name information.

#### Secure Channel Establishment and Maintenance Structures

Structures and enumerated types in this group are used to establish and maintain the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NL\_AUTH\_MESSAGE

The NL\_AUTH\_MESSAGE structure is a token containing information that is part of the first message in establishing a [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) between a client and a server. It is used for establishing the secure session when Netlogon functions as a [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a). For details about NL\_AUTH\_MESSAGE construction, see section [3.3.4.1](#Section_b28a01cb295d4833bdb6b113baf109b4).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| MessageType | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Buffer (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**MessageType (4 bytes):** A 32-bit unsigned integer. This value is used to indicate whether the message is a negotiate request message sent from a client to a server, or a negotiate response message sent from the server to the client. **MessageType** MUST be one, and only one, of the following.

| Value | Meaning |
| --- | --- |
| 0x00000000 | This is a negotiate request message. |
| 0x00000001 | This is a negotiate response message. |

**Flags (4 bytes):** A set of bit flags indicating the [**principal**](#gt_8492780e-99e2-47ba-8553-aedb8de9f9c0) names carried in the request. A flag is TRUE (or set) if its value is equal to 1. These flags are set only in negotiate request messages. The value is constructed from one or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | E | D | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Buffer contains a NetBIOS [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) as an OEM\_STRING ([[MS-CIFS]](%5bMS-CIFS%5d.pdf#Section_d416ff7cc536406ea9514f04b2fd1d2b) section 2.2.1.1). |
| B | Buffer contains a NetBIOS [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b) as an OEM\_STRING ([MS-CIFS] section 2.2.1.1). |
| C | Buffer contains a [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) domain name as a compressed UTF-8 string, as specified in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) section 4.1.4. |
| D | Buffer contains a DNS host name as a compressed UTF-8 string, as specified in [RFC1035] section 4.1.4. |
| E | Buffer contains a NetBIOS computer name as a compressed UTF-8 string, as specified in [RFC1035] section 4.1.4. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**Buffer (variable):** Text buffer that contains a concatenation of null-terminated strings for each of the name flags set in the **Flags** field. The order is the same as the order of the **Flags** values (A–E). This buffer is only used in negotiate request messages. For negotiate response messages, the buffer contains a NULL character.

##### NL\_AUTH\_SIGNATURE

The NL\_AUTH\_SIGNATURE structure is a security token that defines the authentication signature used by Netlogon to execute Netlogon methods over a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca). It follows the security trailer that a [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) MUST associate with a signed or encrypted message. A security trailer or sec\_trailer structure ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.2.11) has syntax equivalent to the auth\_verifier\_co\_t structure, as specified in "Common Authentication Verifier Encodings" in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 13.2.6.1. When Netlogon is functioning as its own SSP for the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) connection, this structure contains the signature, a sequence number, and if encryption is requested, a confounder. See section [3.3.4.2](#Section_2af2dc5f794143aba6d063161a591a6e).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| SignatureAlgorithm | | | | | | | | | | | | | | | | SealAlgorithm | | | | | | | | | | | | | | | |
| Pad | | | | | | | | | | | | | | | | Flags | | | | | | | | | | | | | | | |
| SequenceNumber | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Checksum | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Confounder | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**SignatureAlgorithm (2 bytes):** A 16-bit little-endian integer that identifies the algorithm that is used for signature computation. The only supported signature algorithm is [**HMAC-MD5**](#gt_ba024019-a866-41df-99a5-764b7eab2e1e), as specified in [[RFC2104]](https://go.microsoft.com/fwlink/?LinkId=90314). The **SignatureAlgorithm** field MUST contain the following value.

| Value | Meaning |
| --- | --- |
| 0x0077 | The packet is signed using HMAC-MD5. |

**SealAlgorithm (2 bytes):** A 16-bit little-endian integer that identifies the algorithm used for encryption. The only supported encryption algorithm is RSA-[**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) (for more information about RC4, see [[SCHNEIER]](https://go.microsoft.com/fwlink/?LinkId=817338) section 17.1). The **SealAlgorithm** field MUST contain one of the following values.

| Value | Meaning |
| --- | --- |
| 0xFFFF | The packet is not encrypted. |
| 0x007A | The packet is encrypted using RC4. |

**Pad (2 bytes):** A 2-byte padding field. Both bytes MUST be set to 0xFF.

**Flags (2 bytes):** Specifies properties of the structure. No flags are currently defined. Both bytes MUST be set to zero and MUST be ignored on receipt.

**SequenceNumber (8 bytes):** A 64-bit little-endian integer containing the sequence number of the RPC message. For more details about how to calculate the **SequenceNumber**, see section [3.3.4.2.1](#Section_0593a87c7a83423280f8571e34220fed).

**Checksum (8 bytes):** A 64-bit value containing the final checksum of the signature and the RPC message. For more details about how to calculate the checksum, see section 3.3.4.2.1.

**Confounder (8 bytes):** A buffer used when the structure is used for encryption in addition to signing. The bytes are filled with random data that is used by the encryption algorithm. If the structure is used only for signing, the confounder is not included. For details about the confounder and encrypting the data, see section 3.3.4.2.1.

##### NL\_AUTH\_SHA2\_SIGNATURE

The NL\_AUTH\_SHA2\_SIGNATURE structure is a security token that defines the SHA2 authentication signature that SHOULD[<18>](#Appendix_A_18" \o "Product behavior note 18) be used by Netlogon to execute Netlogon methods over a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca). It follows the security trailer that a [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) MUST associate with a signed or encrypted message. A security trailer or sec\_trailer structure ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.2.11) has syntax equivalent to the auth\_verifier\_co\_t structure, as specified in [[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 13.2.6.1. When Netlogon is functioning as its own SSP for the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) connection, this structure contains the signature, a sequence number, and (if encryption is requested) a confounder. See section [3.3.4.2](#Section_2af2dc5f794143aba6d063161a591a6e).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| SignatureAlgorithm | | | | | | | | | | | | | | | | SealAlgorithm | | | | | | | | | | | | | | | |
| Pad | | | | | | | | | | | | | | | | Flags | | | | | | | | | | | | | | | |
| SequenceNumber | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Checksum (32 bytes) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Confounder | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**SignatureAlgorithm (2 bytes):** A 16-bit little-endian integer that identifies the algorithm that is used for signature computation. The only supported signature algorithm is HMAC-SHA256 [[RFC4634]](https://go.microsoft.com/fwlink/?LinkId=90486). The **SignatureAlgorithm** field MUST contain the following value.

| Value | Meaning |
| --- | --- |
| 0x0013 | The packet is signed using HMAC-SHA256. |

**SealAlgorithm (2 bytes):** A 16-bit little-endian integer that identifies the algorithm used for encryption. The only supported encryption algorithm is AES-128 [[FIPS197]](https://go.microsoft.com/fwlink/?LinkId=89870). The **SealAlgorithm** field MUST contain one of the following values.

| Value | Meaning |
| --- | --- |
| 0xFFFF | The packet is not encrypted. |
| 0x001A | The packet is encrypted using AES-128. |

**Pad (2 bytes):** A 2-byte padding field. Both bytes MUST be set to 0xFF.

**Flags (2 bytes):** Specifies properties of the structure. No **Flags** are currently defined. Both bytes MUST be set to zero and MUST be ignored on receipt.

**SequenceNumber (8 bytes):** A 64-bit little-endian integer containing the sequence number of the RPC message. For more details about how to calculate the **SequenceNumber**, see section [3.3.4.2.1](#Section_0593a87c7a83423280f8571e34220fed).

**Checksum (32 bytes):** A 256-bit value containing the final **Checksum** of the signature and the RPC message. For more details about how to calculate the **Checksum**, see section 3.3.4.2.1.

**Confounder (8 bytes):** A buffer that is employed when the structure is used for encryption, in addition to signing. The bytes are filled with random data that is used by the encryption algorithm. If the structure is used only for signing, the **Confounder** is not included. For details about the **Confounder** and encrypting the data, see section 3.3.4.2.1.

##### NETLOGON\_CREDENTIAL

The NETLOGON\_CREDENTIAL structure contains 8 bytes of data that have two distinct uses: for [**session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation and for building a Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

1. typedef struct \_NETLOGON\_CREDENTIAL {
2. CHAR data[8];
3. } NETLOGON\_CREDENTIAL,
4. \*PNETLOGON\_CREDENTIAL;

**data:**  The meaning of the 8 bytes of data contained in this structure is determined by the following:

* When session-key negotiation is performed, the data field carries an 8-byte challenge. Also see section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9).
* When the NETLOGON\_CREDENTIAL is used as part of a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, the data field carries 8 bytes of encrypted data, as specified in sections [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585) and [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

##### NETLOGON\_LSA\_POLICY\_INFO

The NETLOGON\_LSA\_POLICY\_INFO structure defines [**Local Security Authority (LSA)**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy information as an unsigned character buffer. For details, see [[LSAPOLICY]](https://go.microsoft.com/fwlink/?LinkId=89934) and [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc).

1. typedef struct \_NETLOGON\_LSA\_POLICY\_INFO {
2. ULONG LsaPolicySize;
3. [size\_is(LsaPolicySize)] UCHAR \* LsaPolicy;
4. } NETLOGON\_LSA\_POLICY\_INFO,
5. \*PNETLOGON\_LSA\_POLICY\_INFO;

**LsaPolicySize:**  This field is not used, and is set to zero.

**LsaPolicy:**  This field is not used, and is initialized to NULL.

##### NETLOGON\_WORKSTATION\_INFO

The NETLOGON\_WORKSTATION\_INFO structure defines information passed into the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method, as specified in 3.5.4.4.9. It SHOULD[<19>](#Appendix_A_19" \o "Product behavior note 19) be used to convey information about a member workstation from the client side to the server side.

1. typedef struct \_NETLOGON\_WORKSTATION\_INFO {
2. NETLOGON\_LSA\_POLICY\_INFO LsaPolicy;
3. [string] wchar\_t\* DnsHostName;
4. [string] wchar\_t\* SiteName;
5. [string] wchar\_t\* Dummy1;
6. [string] wchar\_t\* Dummy2;
7. [string] wchar\_t\* Dummy3;
8. [string] wchar\_t\* Dummy4;
9. RPC\_UNICODE\_STRING OsVersion;
10. RPC\_UNICODE\_STRING OsName;
11. RPC\_UNICODE\_STRING DummyString3;
12. RPC\_UNICODE\_STRING DummyString4;
13. ULONG WorkstationFlags;
14. ULONG KerberosSupportedEncryptionTypes;
15. ULONG DummyLong3;
16. ULONG DummyLong4;
17. } NETLOGON\_WORKSTATION\_INFO,
18. \*PNETLOGON\_WORKSTATION\_INFO;

**LsaPolicy:**  A [NETLOGON\_LSA\_POLICY\_INFO](#Section_4676ac8320994e33b680502fd8a32dbd) structure, as specified in section 2.2.1.3.5, that contains the [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy for this [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**DnsHostName:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) host name of the client.

**SiteName:**  A null-terminated Unicode string that contains the name of the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) where the workstation resides.

**Dummy1:**  MUST be set to NULL and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**Dummy2:**  MUST be set to NULL and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**Dummy3:**  MUST be set to NULL and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**Dummy4:**  MUST be set to NULL and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**OsVersion:**  An RPC\_UNICODE\_STRING structure (as defined in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10) in which the **Length** and **MaximumLength** fields are set to the size of an OSVERSIONINFOEX structure and the **Buffer** field points to an OSVERSIONINFOEX ([[MS-RPRN]](%5bMS-RPRN%5d.pdf#Section_d42db7d5f14144668f470a4be14e2fc1) section 2.2.3.10.2) structure. *OsVersion* contains the version number of the operating system installed on the client machine.

**OsName:**  A null-terminated Unicode string that SHOULD[<20>](#Appendix_A_20" \o "Product behavior note 20) contain the name of the operating system installed on the client machine. The [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) that receives this data structure updates the **operatingSystem** attribute of the client's machine account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90), as specified in [[MS-ADA3]](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0) section 2.53.

**DummyString3:**  A STRING structure, defined in section [2.2.1.1.1](#Section_56a8d298dbeb4eb5ad9876536ec352f8), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyString4:**  See description for DummyString3.

**WorkstationFlags:**  A set of bit flags specifying workstation behavior. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Client will receive inbound [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.7.9. The client sets this bit in order to receive the inbound trusts. |
| B | Client handles the update of the [**service principal name (SPN)**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4). |

All other bits MUST be set to zero and MUST be ignored on receipt.

**KerberosSupportedEncryptionTypes:**  The **msDS-SupportedEncryptionTypes** attribute of the client's machine account object in Active Directory, as specified in [[MS-ADA2]](%5bMS-ADA2%5d.pdf#Section_e20ebc4e528540bab3bdffcb81c2783e) section 2.464.[<21>](#Appendix_A_21" \o "Product behavior note 21)

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

##### NL\_TRUST\_PASSWORD

The NL\_TRUST\_PASSWORD structure defines a buffer for carrying a computer account password, or a [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password, to be transmitted over the wire. It SHOULD[<22>](#Appendix_A_22" \o "Product behavior note 22) be transported as an input parameter to the [NetrServerPasswordSet2](#Section_14b020a80bcf4af5ab72cc92bc6b1d81) method, as specified in section 3.5.4.4.5. [**Domain members**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) use NetrServerPasswordSet2 to change their computer account password. The [**primary domain controller**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) uses NetrServerPasswordSet2 to change trust passwords for all directly trusted [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). The NL\_TRUST\_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire.

1. typedef struct \_NL\_TRUST\_PASSWORD {
2. WCHAR Buffer[256];
3. ULONG Length;
4. } NL\_TRUST\_PASSWORD,
5. \*PNL\_TRUST\_PASSWORD;

**Buffer:**  Array of [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) characters that is treated as a byte buffer containing the password, as follows:

* For a computer account password, the buffer has the following format:

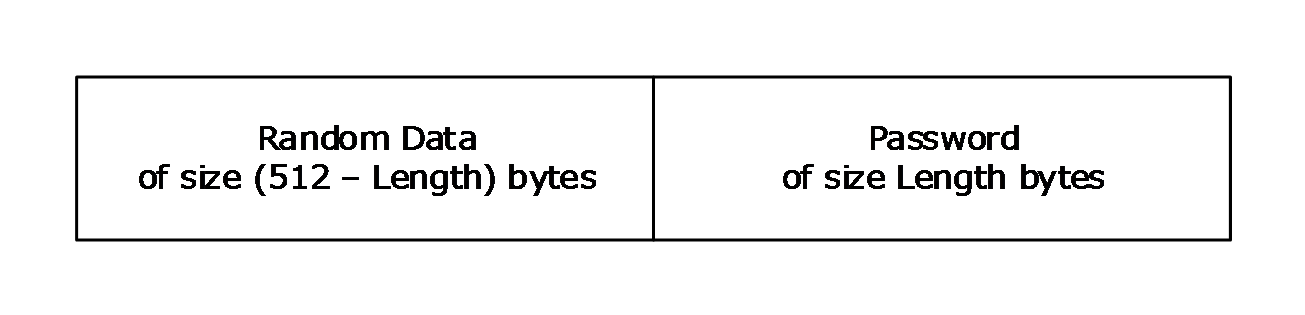
****

Figure 4: Computer account password buffer format

The first (512 – Length) bytes MUST be randomly generated data that serves as an additional source of entropy during encryption. The last Length bytes of the buffer MUST contain the clear text password.

* For a domain trust password, the buffer has the following format:

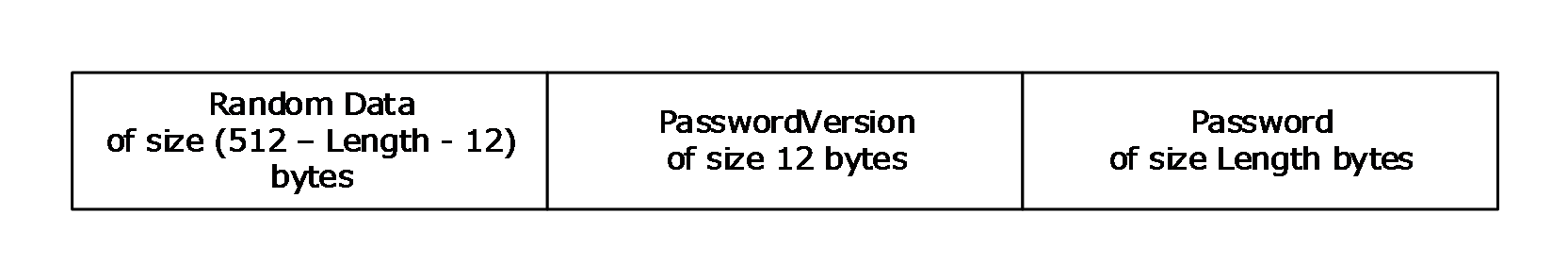


Figure 5: Domain trust password buffer format

The last Length bytes of the buffer contain the clear text password. The 12 bytes preceding the password are filled with the password version information as defined below. The rest of the buffer is filled with randomly generated data.

* The **PasswordVersion** part of the preceding diagram has the following format:

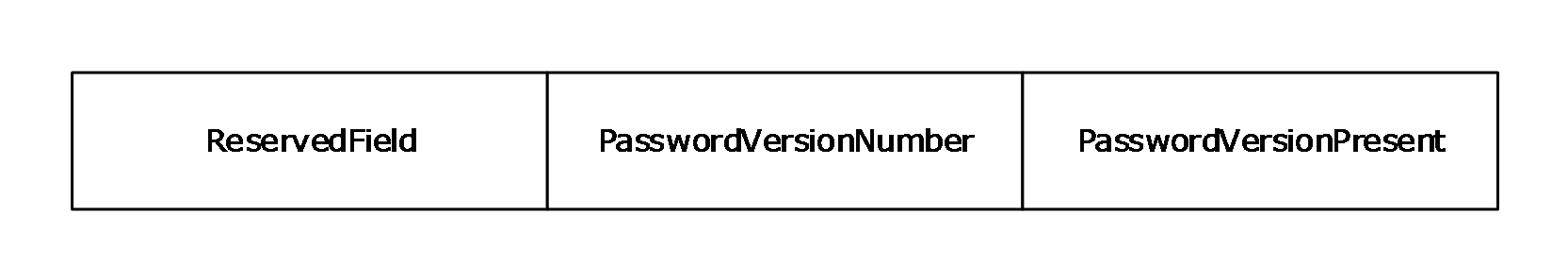


Figure 6: Password version buffer format

Where **ReservedField**, **PasswordVersionNumber**, and **PasswordVersionPresent** are the fields of the [NL\_PASSWORD\_VERSION](#Section_cba0e87eb91f411b9be86fd321e126b7) structure, as specified in section 2.2.1.3.8. The **PasswordVersionPresent** field is used to indicate whether the buffer contains a computer account password or a trust password: If the value of the **PasswordVersionPresent** field is 0x02231968, then the buffer contains a trust password; otherwise the buffer contains a computer account password.

**Length:**  The length of the password, in bytes.

##### NL\_PASSWORD\_VERSION

The NL\_PASSWORD\_VERSION structure defines a password version number that is used to distinguish between different versions of information passed in the **Buffer** field of the [NL\_TRUST\_PASSWORD](#Section_52d5bd865caf47aaaae4cadf7339ec83) structure. The NL\_PASSWORD\_VERSION structure SHOULD[<23>](#Appendix_A_23" \o "Product behavior note 23) be prepended to the password in the buffer of NL\_TRUST\_PASSWORD. This structure is only used for interdomain [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) accounts.

1. typedef struct \_NL\_PASSWORD\_VERSION {
2. ULONG ReservedField;
3. ULONG PasswordVersionNumber;
4. ULONG PasswordVersionPresent;
5. } NL\_PASSWORD\_VERSION,
6. \*PNL\_PASSWORD\_VERSION;

**ReservedField:**  MUST be set to zero when sent and MUST be ignored on receipt.

**PasswordVersionNumber:**  Integer value that contains the current password version number. The password version number is incremented by one when a new password is generated; the value for the first password is one.

**PasswordVersionPresent:**  MUST be 0x02231968, which is a constant used to indicate that the password version number is present and is stored in **PasswordVersionNumber**. This member is relevant only for server-to-server communication.

##### NETLOGON\_WORKSTATION\_INFORMATION

The NETLOGON\_WORKSTATION\_INFORMATION union SHOULD[<24>](#Appendix_A_24" \o "Product behavior note 24) select between two parameters of type [NETLOGON\_WORKSTATION\_INFO](#Section_3ae9e9a9a3034fa58e11823d9e7e1e61) structure, as specified in section 2.2.1.3.6, based on the value of the *Level* parameter of the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method, as specified in section 3.5.4.4.9.

1. typedef
2. [switch\_type(DWORD)]
3. union \_NETLOGON\_WORKSTATION\_INFORMATION {
4. [case(1)]
5. PNETLOGON\_WORKSTATION\_INFO WorkstationInfo;
6. [case(2)]
7. PNETLOGON\_WORKSTATION\_INFO LsaPolicyInfo;
8. } NETLOGON\_WORKSTATION\_INFORMATION,
9. \*PNETLOGON\_WORKSTATION\_INFORMATION;

**WorkstationInfo:**  Field is selected when the switched DWORD ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.2.9) constant is 0x00000001.

**LsaPolicyInfo:**  Field is selected when the switched DWORD constant is 0x00000002.

##### NETLOGON\_ONE\_DOMAIN\_INFO

The NETLOGON\_ONE\_DOMAIN\_INFO structure SHOULD[<25>](#Appendix_A_25" \o "Product behavior note 25) define information about a single [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). It is in turn contained in the [NETLOGON\_DOMAIN\_INFO](#Section_440c3430ed5f481db60274db422df3c8) structure, as specified in section 2.2.1.3.11. The NETLOGON\_DOMAIN\_INFO structure describes domain relationships and is generated as output from the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method, as specified in section 3.5.4.4.9.

1. typedef struct \_NETLOGON\_ONE\_DOMAIN\_INFO {
2. RPC\_UNICODE\_STRING DomainName;
3. RPC\_UNICODE\_STRING DnsDomainName;
4. RPC\_UNICODE\_STRING DnsForestName;
5. GUID DomainGuid;
6. PRPC\_SID DomainSid;
7. RPC\_UNICODE\_STRING TrustExtension;
8. RPC\_UNICODE\_STRING DummyString2;
9. RPC\_UNICODE\_STRING DummyString3;
10. RPC\_UNICODE\_STRING DummyString4;
11. ULONG DummyLong1;
12. ULONG DummyLong2;
13. ULONG DummyLong3;
14. ULONG DummyLong4;
15. } NETLOGON\_ONE\_DOMAIN\_INFO,
16. \*PNETLOGON\_ONE\_DOMAIN\_INFO;

**DomainName:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the domain being described. This field MUST NOT be an empty string.

**DnsDomainName:**  A null-terminated Unicode string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) for this domain. This field MUST NOT be an empty string.

**DnsForestName:**  A null-terminated Unicode string that contains the DNS [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) name for this domain.

**DomainGuid:**  A globally unique 128-bit identifier for this domain.

**DomainSid:**  The [**security identifier (SID)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d), as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.2.3 for this domain.

**TrustExtension:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, which does not point to a Unicode string, but in fact points to a buffer of size 16, in bytes, in the following format.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| Flags | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ParentIndex | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TrustType | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TrustAttributes | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

This structure is supplementary domain [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) information that contains the following fields of a [DS\_DOMAIN\_TRUSTSW](#Section_7de9866ed3ef4a9f98a5c2dcff1e61c1) structure: **Flags**, **ParentIndex**, **TrustType**, and **TrustAttributes**. For more details on usage in NetrLogonGetDomainInfo, see section 3.5.4.4.9. For more details on the DS\_DOMAIN\_TRUSTSW structure, see section 2.2.1.6.2.

**DummyString2:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString3:**  See description for DummyString2.

**DummyString4:**  See description for DummyString2.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

##### NETLOGON\_DOMAIN\_INFO

The NETLOGON\_DOMAIN\_INFO structure SHOULD[<26>](#Appendix_A_26" \o "Product behavior note 26) define information returned as output from the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method, as specified in section 3.5.4.4.9. It contains information about a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), including naming information and a list of [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domains.

1. typedef struct \_NETLOGON\_DOMAIN\_INFO {
2. NETLOGON\_ONE\_DOMAIN\_INFO PrimaryDomain;
3. ULONG TrustedDomainCount;
4. [size\_is(TrustedDomainCount)] PNETLOGON\_ONE\_DOMAIN\_INFO TrustedDomains;
5. NETLOGON\_LSA\_POLICY\_INFO LsaPolicy;
6. RPC\_UNICODE\_STRING DnsHostNameInDs;
7. RPC\_UNICODE\_STRING DummyString2;
8. RPC\_UNICODE\_STRING DummyString3;
9. RPC\_UNICODE\_STRING DummyString4;
10. ULONG WorkstationFlags;
11. ULONG SupportedEncTypes;
12. ULONG DummyLong3;
13. ULONG DummyLong4;
14. } NETLOGON\_DOMAIN\_INFO,
15. \*PNETLOGON\_DOMAIN\_INFO;

**PrimaryDomain:**  A [NETLOGON\_ONE\_DOMAIN\_INFO](#Section_77cd977686124dab9748bfb07247fd4c) structure, as specified in section 2.2.1.3.10, that contains information about the domain of which the server is a member.

**TrustedDomainCount:**  The number of trusted domains listed in TrustedDomains.

**TrustedDomains:**  A pointer to an array of NETLOGON\_ONE\_DOMAIN\_INFO structures, as specified in section 2.2.1.3.10, which contain information about domains with which the current domain has a trust relationship.

**LsaPolicy:**  A [NETLOGON\_LSA\_POLICY\_INFO](#Section_4676ac8320994e33b680502fd8a32dbd) data structure that contains the [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy for this domain. This field is not used. For details, see section 2.2.1.3.5.

**DnsHostNameInDs:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) host name for the client.

**DummyString2:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString3:**  See description for DummyString2.

**DummyString4:**  See description for DummyString2.

**WorkstationFlags:**  A set of bit flags that specify workstation behavior. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Client receives inbound trusts. |
| B | Client handles the update of the [**service principal name (SPN)**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4). See [[SPNNAMES]](https://go.microsoft.com/fwlink/?LinkId=90532) for details. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**SupportedEncTypes:**  A set of bit flags that SHOULD[<27>](#Appendix_A_27" \o "Product behavior note 27) specify the encryption types supported, as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.7.18. See [MS-LSAD] for a specification of these bit values and their allowed combinations.

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

##### NETLOGON\_DOMAIN\_INFORMATION

The NETLOGON\_DOMAIN\_INFORMATION union SHOULD[<28>](#Appendix_A_28" \o "Product behavior note 28) select either a [NETLOGON\_DOMAIN\_INFO](#Section_440c3430ed5f481db60274db422df3c8), as specified in section 2.2.1.3.11, or a [NETLOGON\_LSA\_POLICY\_INFO](#Section_4676ac8320994e33b680502fd8a32dbd), as specified in section 2.2.1.3.5, data type based on the value of the *Level* parameter to the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method, as specified in section 3.5.4.4.9.

1. typedef
2. [switch\_type(DWORD)]
3. union \_NETLOGON\_DOMAIN\_INFORMATION {
4. [case(1)]
5. PNETLOGON\_DOMAIN\_INFO DomainInfo;
6. [case(2)]
7. PNETLOGON\_LSA\_POLICY\_INFO LsaPolicyInfo;
8. } NETLOGON\_DOMAIN\_INFORMATION,
9. \*PNETLOGON\_DOMAIN\_INFORMATION;

**DomainInfo:** This field is selected when the switched DWORD ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.2.9) value is set to 0x00000001. The union contains a NETLOGON\_DOMAIN\_INFO structure, as specified in section 2.2.1.3.11.

**LsaPolicyInfo:**  This field is selected when the switched DWORD value is set to 0x00000002. The union contains a NETLOGON\_LSA\_POLICY\_INFO structure, as specified in section 2.2.1.3.5.

##### NETLOGON\_SECURE\_CHANNEL\_TYPE

The NETLOGON\_SECURE\_CHANNEL\_TYPE enumeration specifies the type of [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to use in a logon transaction.

1. typedef enum \_NETLOGON\_SECURE\_CHANNEL\_TYPE
2. {
3. NullSecureChannel = 0,
4. MsvApSecureChannel = 1,
5. WorkstationSecureChannel = 2,
6. TrustedDnsDomainSecureChannel = 3,
7. TrustedDomainSecureChannel = 4,
8. UasServerSecureChannel = 5,
9. ServerSecureChannel = 6,
10. CdcServerSecureChannel = 7
11. } NETLOGON\_SECURE\_CHANNEL\_TYPE;

**NullSecureChannel:** An unauthenticated channel type. This value MUST NOT be used in the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) calls between a client and a remote server. The error code STATUS\_INVALID\_PARAMETER SHOULD be returned.

**MsvApSecureChannel:** A secure channel between the local [**NT LAN Manager (NTLM)**](#gt_6e52bc15-d369-45fd-b098-d51fc9baa56a) [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) and the Netlogon server. The client and the server are the same machine for this channel type. This value MUST NOT be used in the Netlogon RPC calls between a client and a remote server. The error code STATUS\_INVALID\_PARAMETER SHOULD be returned.

**WorkstationSecureChannel:** A secure channel from a [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) to a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**TrustedDnsDomainSecureChannel:** A secure channel between two DCs, connected through a [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) relationship created between two [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). A [**trusted domain object (TDO)**](#gt_f2ceef4e-999b-4276-84cd-2e2829de5fc4) is used in this type of channel.

**TrustedDomainSecureChannel:** A secure channel between two DCs, connected through a trust relationship created between two domains.[<29>](#Appendix_A_29" \o "Product behavior note 29)

**UasServerSecureChannel:** Secure channel from a LAN Manager server to a DC. This value is no longer supported, and it MUST NOT be used in the Netlogon RPC calls between a client and a remote server. The error code STATUS\_INVALID\_PARAMETER SHOULD be returned.

**ServerSecureChannel:** A secure channel from a [**backup domain controller**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3) to a [**primary domain controller**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d).

**CdcServerSecureChannel: A** secure channel from a [**read-only domain controller (RODC)**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to a domain controller.[<30>](#Appendix_A_30" \o "Product behavior note 30)

##### NETLOGON\_CAPABILITIES

The NETLOGON\_CAPABILITIES union SHOULD[<31>](#Appendix_A_31" \o "Product behavior note 31) carry the supported Netlogon capabilities.

1. typedef
2. [switch\_type(DWORD)]
3. union \_NETLOGON\_CAPABILITIES {
4. [case(1)]
5. ULONG ServerCapabilities;
6. } NETLOGON\_CAPABILITIES,
7. \*PNETLOGON\_CAPABILITIES;

**ServerCapabilities:**  A 32-bit set of bit flags that identify the server's capabilities (section [3.5.4.4.10](#Section_5780fc6c82f0489fb9a0a9e855388492)).

##### NL\_OSVERSIONINFO\_V1

The NL\_OSVERSIONINFO\_V1 structure specifies the values used to update the **operatingSystemVersion** and **operatingSystem** attributes on the client's computer account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) on a normal (writable) [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).[<32>](#Appendix_A_32" \o "Product behavior note 32)

1. typedef struct \_NL\_OSVERSIONINFO\_V1 {
2. DWORD dwOSVersionInfoSize;
3. DWORD dwMajorVersion;
4. DWORD dwMinorVersion;
5. DWORD dwBuildNumber;
6. DWORD dwPlatformId;
7. wchar\_t szCSDVersion[128];
8. USHORT wServicePackMajor;
9. USHORT wServicePackMinor;
10. USHORT wSuiteMask;
11. UCHAR wProductType;
12. UCHAR wReserved;
13. } NL\_OSVERSIONINFO\_V1;

**dwOSVersionInfoSize:**  The size, in bytes, of this data structure. Set this member to sizeof(NL\_OSVERSIONINFO\_V1).

**dwMajorVersion:**  The implementation-specific major version number of the operating system.[<33>](#Appendix_A_33" \o "Product behavior note 33)

**dwMinorVersion:**  The implementation-specific minor version number of the operating system.[<34>](#Appendix_A_34" \o "Product behavior note 34)

**dwBuildNumber:**  The build number of the operating system.

**dwPlatformId:**  The operating system platform. This member can be 0x00000002.

**szCSDVersion:**  A null-terminated string, such as "Service Pack 3", that indicates the latest service pack installed on the system. If no service pack has been installed, the string is empty.

**wServicePackMajor:**  The major version number of the latest service pack installed on the system. For example, for "Service Pack 3", the major version number is 3. If no service pack has been installed, the value is 0.

**wServicePackMinor:**  The minor version number of the latest service pack installed on the system. For example, for "Service Pack 3", the minor version number is 0.

**wProductType:**  Any additional information about the system. This member can be one of the following values.

| Value | Meaning |
| --- | --- |
| VER\_NT\_DOMAIN\_CONTROLLER  0x00000002 | The system is a DC. |
| VER\_NT\_SERVER  0x00000003 | The system is a server. Note that a server that is also a DC is reported as VER\_NT\_DOMAIN\_CONTROLLER, not VER\_NT\_SERVER. |
| VER\_NT\_WORKSTATION  0x00000001 | Identifies the operating system.[<35>](#Appendix_A_35" \o "Product behavior note 35) |

**wReserved:** Reserved for future use.[<36>](#Appendix_A_36" \o "Product behavior note 36)

##### NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1

The NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 structure specifies the values to update on the client's computer account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) on a normal (writable) [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).[<37>](#Appendix_A_37" \o "Product behavior note 37)

1. typedef struct \_NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 {
2. [unique, string] wchar\_t\* ClientDnsHostName;
3. [unique] NL\_OSVERSIONINFO\_V1\* OsVersionInfo\_V1;
4. [unique, string] wchar\_t\* OsName;
5. } NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1;

**ClientDnsHostName:**  A NULL or null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that is used to update the attribute **dNSHostName** on the client's computer account object in Active Directory.

**OsVersionInfo\_V1:**  If not NULL, the attribute **operatingSystemVersion** on the client's computer account in Active Directory (using the ABNF Syntax as specified in [[RFC2234]](https://go.microsoft.com/fwlink/?LinkId=90323)) is set to:

* If OsVersionInfo\_V1.dwBuildNumber is 0:

1. operatingSystemVersion = MajorVersion "." MinorVersion
2. MajorVersion = OsVersionInfo\_V1.dwMajorVersion
3. MinorVersion = OsVersionInfo\_V1.dwMinorVersion

* Otherwise:

1. operatingSystemVersion = MajorVersion "." MinorVersion "."
2. BuildNumber
3. MajorVersion = OsVersionInfo\_V1.dwMajorVersion
4. MinorVersion = OsVersionInfo\_V1.dwMinorVersion
5. BuildNumber = OsVersionInfo\_V1.dwBuildNumber

**OsName:**  A NULL or a null-terminated Unicode string that SHOULD[<38>](#Appendix_A_38" \o "Product behavior note 38) be used to update the attribute **operatingSystem** on the client's computer account object in Active Directory.

##### NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES

The NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES union defines versioning.

1. typedef
2. [switch\_type(DWORD)]
3. union {
4. [case(1)]
5. NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 V1;
6. } NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES;

**V1:**  An [NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 (section 2.2.1.3.16)](#Section_f4ed8790d7e84ca18062d25784ed79e3) structure.[<39>](#Appendix_A_39" \o "Product behavior note 39)

##### NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1

The NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 structure SHOULD[<40>](#Appendix_A_40" \o "Product behavior note 40) specify the values returned from the normal (writable) [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

1. typedef struct \_NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 {
2. [unique, string] wchar\_t\* HubName;
3. [unique, string] wchar\_t\*\* OldDnsHostName;
4. [unique] ULONG \* SupportedEncTypes;
5. } NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1;

**HubName:**  The [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the [**writable domain controller**](#gt_9d964ddb-09d6-4a1b-b27b-42adabc07993) receiving [NetrChainSetClientAttributes (section 3.5.4.4.11)](#Section_3a416e8202994ff0a25d223f972ba1d6). The [**read-only domain controller (RODC)**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) that invoked the method NetrChainSetClientAttributes SHOULD[<41>](#Appendix_A_41" \o "Product behavior note 41) attempt to replicate the computer account object from **HubName** to itself, ignoring errors.

**OldDnsHostName:**  The client's [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) host name, if any, from the **dNSHostName** attribute  
([[MS-ADA1]](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f) section 2.185) on the client's computer account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) on the writable domain controller. If there was an update to the **dNSHostName** attribute by the writable domain controller as a result of receiving NetrChainSetClientAttributes, this value will hold the previous value of that attribute.

**SupportedEncTypes:**  The supported encryption algorithms received from the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) request, in the **SupportedEncTypes** field in the [NETLOGON\_DOMAIN\_INFO (section 2.2.1.3.11)](#Section_440c3430ed5f481db60274db422df3c8) structure.[<42>](#Appendix_A_42" \o "Product behavior note 42)

##### NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES

The NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES union defines versioning. Currently, only version 1 is supported.

1. typedef
2. [switch\_type(DWORD)]
3. union {
4. [case(1)]
5. NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 V1;
6. } NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES;

**V1:**  An [NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 (section 2.2.1.3.18)](#Section_ab43a76224e245c387011838589d80fe) structure.[<43>](#Appendix_A_43" \o "Product behavior note 43)

#### Pass-Through Authentication Structures

Structures and enumerated types in this group are used for generic pass-though and for user logon and logoff, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### LM\_CHALLENGE

The LM\_CHALLENGE structure carries a LAN Manager authentication challenge.

1. typedef struct {
2. CHAR data[8];
3. } LM\_CHALLENGE;

**data:**   A string of eight characters that contains a LAN Manager authentication challenge, which is an unencrypted [**nonce**](#gt_001c0e40-0980-417d-853c-f7cb34ba6d3b).

For more information, see [[LANMAN]](https://go.microsoft.com/fwlink/?LinkId=89929).

##### NETLOGON\_GENERIC\_INFO

The NETLOGON\_GENERIC\_INFO structure defines a structure that contains logon information in binary format. Authentication protocols make use of this structure for passing generic logon data through the Netlogon [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that contains the user account to use the domain's [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). For an example of using the NETLOGON\_GENERIC\_INFO structure, see any of the examples documented in [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e).

1. typedef struct \_NETLOGON\_GENERIC\_INFO {
2. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
3. RPC\_UNICODE\_STRING PackageName;
4. ULONG DataLength;
5. [size\_is(DataLength)] UCHAR \* LogonData;
6. } NETLOGON\_GENERIC\_INFO,
7. \*PNETLOGON\_GENERIC\_INFO;

**Identity:**  The [NETLOGON\_LOGON\_IDENTITY\_INFO](#Section_81c44fa00a2741b3b607de39cce7ea1d) structure, as specified in section 2.2.1.4.15, contains information about the logon identity. The **LogonDomainName** field of the NETLOGON\_LOGON\_IDENTITY\_INFO structure indicates the target domain that contains the user account.

**PackageName:**  Contains the name of the [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333), such as Kerberos, to which the data will be delivered on the domain controller in the target domain that was specified in the **Identity** field. This name MUST match the name of an existing security provider; otherwise, the [**Security Support Provider Interface (SSPI)**](#gt_fb216516-748b-4873-8bdd-64c5f4da9920) ([[SSPI]](https://go.microsoft.com/fwlink/?LinkId=90536)) returns a package not found error.

**DataLength:**  The length, in bytes, of **LogonData**.

**LogonData:**  A pointer to a block of binary data that contains the information to be sent to the security package referenced in **PackageName**. This data is opaque to Netlogon.

##### NETLOGON\_INTERACTIVE\_INFO

The NETLOGON\_INTERACTIVE\_INFO structure defines information about an [**interactive logon**](#gt_9360639b-135c-46dc-9f9e-85728008146f) instance.

1. typedef struct \_NETLOGON\_INTERACTIVE\_INFO {
2. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
3. LM\_OWF\_PASSWORD LmOwfPassword;
4. NT\_OWF\_PASSWORD NtOwfPassword;
5. } NETLOGON\_INTERACTIVE\_INFO,
6. \*PNETLOGON\_INTERACTIVE\_INFO;

**Identity:**  A [NETLOGON\_LOGON\_IDENTITY\_INFO](#Section_81c44fa00a2741b3b607de39cce7ea1d) structure, as specified in section 2.2.1.4.15, that contains information about the logon identity.

**LmOwfPassword:**  An [LM\_OWF\_PASSWORD](#Section_30a12be7a4ed4ef2bd8883961edb8f26) structure, as specified in section 2.2.1.1.3, that contains the LMOWFv1 of a password. LMOWFv1 is specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1.

**NtOwfPassword:**  An [NT\_OWF\_PASSWORD](#Section_f7458576d53847cdb387b6f98449a0ee) structure, as specified in section 2.2.1.1.4, that contains the NTOWFv1 of a password. NTOWFv1 is specified in NTLM v1 Authentication in [MS-NLMP] section 3.3.1.

##### NETLOGON\_SERVICE\_INFO

The NETLOGON\_SERVICE\_INFO structure defines information about a service account logon. Operating system services use service accounts as their run-time security identity.

1. typedef struct \_NETLOGON\_SERVICE\_INFO {
2. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
3. LM\_OWF\_PASSWORD LmOwfPassword;
4. NT\_OWF\_PASSWORD NtOwfPassword;
5. } NETLOGON\_SERVICE\_INFO,
6. \*PNETLOGON\_SERVICE\_INFO;

**Identity:**  [NETLOGON\_LOGON\_IDENTITY\_INFO](#Section_81c44fa00a2741b3b607de39cce7ea1d) structure, as specified in section 2.2.1.4.15, that contains information about the logon identity.

**LmOwfPassword:**  [LM\_OWF\_PASSWORD](#Section_30a12be7a4ed4ef2bd8883961edb8f26) structure, as specified in section 2.2.1.1.3, that contains the LMOWFv1 of a password. LMOWFv1 is specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1.

**NtOwfPassword:**  [NT\_OWF\_PASSWORD](#Section_f7458576d53847cdb387b6f98449a0ee) structure, as specified in section 2.2.1.1.4, that contains the NTOWFv1 of a password. NTOWFv1 is specified in NTLM v1 Authentication in [MS-NLMP] section 3.3.1.

##### NETLOGON\_NETWORK\_INFO

The NETLOGON\_NETWORK\_INFO structure defines information that describes a network account logon.

1. typedef struct \_NETLOGON\_NETWORK\_INFO {
2. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
3. LM\_CHALLENGE LmChallenge;
4. STRING NtChallengeResponse;
5. STRING LmChallengeResponse;
6. } NETLOGON\_NETWORK\_INFO,
7. \*PNETLOGON\_NETWORK\_INFO;

**Identity:**  [NETLOGON\_LOGON\_IDENTITY\_INFO](#Section_81c44fa00a2741b3b607de39cce7ea1d) structure, as specified in section 2.2.1.4.15, that contains information about the logon identity.

**LmChallenge:**  [LM\_CHALLENGE](#Section_bb8eca9041bc4ca48419defdf043e01b) structure, as specified in section 2.2.1.4.1, that contains the network authentication challenge. For details about challenges, see [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4).

**NtChallengeResponse:**  String that contains the NT response (see [MS-NLMP]) to the network authentication challenge.

**LmChallengeResponse:**  String that contains the LAN Manager response (see [MS-NLMP]) to the network authentication challenge.

##### NETLOGON\_LEVEL

The NETLOGON\_LEVEL union defines a union of all types of logon information.

1. typedef
2. [switch\_type(NETLOGON\_LOGON\_INFO\_CLASS)]
3. union \_NETLOGON\_LEVEL {
4. [case(NetlogonInteractiveInformation)]
5. PNETLOGON\_INTERACTIVE\_INFO LogonInteractive;
6. [case(NetlogonInteractiveTransitiveInformation)]
7. PNETLOGON\_INTERACTIVE\_INFO LogonInteractiveTransitive;
8. [case(NetlogonServiceInformation)]
9. PNETLOGON\_SERVICE\_INFO LogonService;
10. [case(NetlogonServiceTransitiveInformation)]
11. PNETLOGON\_SERVICE\_INFO LogonServiceTransitive;
12. [case(NetlogonNetworkInformation)]
13. PNETLOGON\_NETWORK\_INFO LogonNetwork;
14. [case(NetlogonNetworkTransitiveInformation)]
15. PNETLOGON\_NETWORK\_INFO LogonNetworkTransitive;
16. [case(NetlogonGenericInformation)]
17. PNETLOGON\_GENERIC\_INFO LogonGeneric;
18. [default]  ;
19. } NETLOGON\_LEVEL,
20. \*PNETLOGON\_LEVEL;

**LogonInteractive:**  This field is selected when the logon information type is **NetlogonInteractiveInformation**. The data type is [NETLOGON\_INTERACTIVE\_INFO](#Section_af76351fef6946bca451e4c4b99bac4a), as specified in section 2.2.1.4.3.

**LogonInteractiveTransitive:**  This field is selected when the logon information type is **NetlogonInteractiveTransitiveInformation**. The data type is NETLOGON\_INTERACTIVE\_INFO, as specified in section 2.2.1.4.3.

**LogonService:**  This field is selected when the logon information type is **NetlogonServiceInformation**. The data type is [NETLOGON\_SERVICE\_INFO](#Section_1c9f2af2e16445489428eae68a03537e), as specified in section 2.2.1.4.4.

**LogonServiceTransitive:**  This field is selected when the logon information type is **NetlogonServiceTransitiveInformation**. The data type is NETLOGON\_SERVICE\_INFO, as specified in section 2.2.1.4.4.

**LogonNetwork:**  This field is selected when the logon information type is **NetlogonNetworkInformation**. The data type is [NETLOGON\_NETWORK\_INFO](#Section_e17b03b8c1d243a198dbcf8d05b9c6a8), as specified in section 2.2.1.4.5.

**LogonNetworkTransitive:**  This field is selected when the logon information type is **NetlogonNetworkTransitiveInformation**. The data type is NETLOGON\_NETWORK\_INFO, as specified in section 2.2.1.4.5.

**LogonGeneric:**  This field is selected when the logon information type is **NetlogonGenericInformation**. The data type is [NETLOGON\_GENERIC\_INFO](#Section_c03d6d959b5e43299645eedcdd167f6e), as specified in section 2.2.1.4.2.

##### NETLOGON\_SID\_AND\_ATTRIBUTES

The NETLOGON\_SID\_AND\_ATTRIBUTES structure contains a [**security identifier (SID)**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) and its attributes.

1. typedef struct \_NETLOGON\_SID\_AND\_ATTRIBUTES {
2. PRPC\_SID Sid;
3. ULONG Attributes;
4. } NETLOGON\_SID\_AND\_ATTRIBUTES,
5. \*PNETLOGON\_SID\_AND\_ATTRIBUTES;

**Sid:**  A pointer to a security identifier (SID).

**Attributes:**  A set of bit flags that contains the set of security attributes assigned to this SID. A bit is TRUE (or set) if its value is equal to 1. The value is constructed from one or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | D | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | The SID cannot have the **SE\_GROUP\_ENABLED** attribute removed. Corresponds to the SID attribute **SE\_GROUP\_MANDATORY**. This attribute prevents the user from disabling the [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac). Disabling a group causes the group to be ignored by access validation routines. |
| B | The SID is enabled by default (as opposed to being enabled by an application). Corresponds to the SID attribute **SE\_GROUP\_ENABLED\_BY\_DEFAULT**. |
| C | The SID is enabled for access checks. Corresponds to the SID attribute **SE\_GROUP\_ENABLED**. |
| D | This group is a [**domain local group**](#gt_32226492-3c8c-4a99-a0d1-f27aaeec3c97). Corresponds to **SE\_GROUP\_RESOURCE**. |

All other bits MUST be set to zero and MUST be ignored on receipt. For more information, see [[SIDATT]](https://go.microsoft.com/fwlink/?LinkId=90515).

These values are opaque to the Netlogon protocol. They are not used or processed directly. All fields of this structure have the same meaning as the identically named fields in the **KERB\_SID\_AND\_ATTRIBUTES** structure as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section 2.2.1.

##### NETLOGON\_VALIDATION\_GENERIC\_INFO2

The NETLOGON\_VALIDATION\_GENERIC\_INFO2 structure defines a structure that contains account information in binary format. This structure is used by authentication protocols to return generic account information upon successful logon validation. For an example of using the NETLOGON\_VALIDATION\_GENERIC\_INFO2 structure, see any of the examples in [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e).

1. typedef struct \_NETLOGON\_VALIDATION\_GENERIC\_INFO2 {
2. ULONG DataLength;
3. [size\_is(DataLength)] UCHAR \* ValidationData;
4. } NETLOGON\_VALIDATION\_GENERIC\_INFO2,
5. \*PNETLOGON\_VALIDATION\_GENERIC\_INFO2;

**DataLength:**  An integer value that contains the length of the data referenced by **ValidationData**, in bytes.

**ValidationData:**  A pointer to a buffer that contains the logon validation information.

##### USER\_SESSION\_KEY

The USER\_SESSION\_KEY structure defines an encrypted user [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d).

1. typedef struct \_USER\_SESSION\_KEY {
2. CYPHER\_BLOCK data[2];
3. } USER\_SESSION\_KEY,
4. \*PUSER\_SESSION\_KEY;

**data:**  A two-element [CYPHER\_BLOCK](#Section_56a8d298dbeb4eb5ad9876536ec352f8) structure, as specified in section 2.2.1.1.1, that contains the 16-byte encrypted user session key.

##### GROUP\_MEMBERSHIP

The GROUP\_MEMBERSHIP structure identifies the [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) to which an account belongs.

1. typedef struct \_GROUP\_MEMBERSHIP {
2. ULONG RelativeId;
3. ULONG Attributes;
4. } GROUP\_MEMBERSHIP,
5. \*PGROUP\_MEMBERSHIP;

**RelativeId:**  The [**relative identifier (RID)**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) for a particular group.

**Attributes:**   A set of values that describe the group membership attributes set for the RID specified in **RelativeId**. The value is constructed from one or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) cannot have the **SE\_GROUP\_ENABLED** attribute removed. Corresponds to the SID attribute **SE\_GROUP\_MANDATORY**. This attribute prevents the user from disabling the group. Disabling a group causes the group to be ignored by access validation routines. |
| B | The SID is enabled by default (as opposed to being enabled by an application). Corresponds to the SID attribute **SE\_GROUP\_ENABLED\_BY\_DEFAULT**. |
| C | The SID is enabled for access checks. Corresponds to the SID attribute **SE\_GROUP\_ENABLED**. The **SE\_GROUP\_ENABLED** attribute enables the group. |

All other bits MUST be zero and MUST be ignored on receipt. For more information, see [[SIDATT]](https://go.microsoft.com/fwlink/?LinkId=90515).

These values are opaque to the Netlogon protocol. They are not used or processed directly. All fields of this structure have the same meaning as the identically named fields in the **GROUP\_MEMBERSHIP** structure as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section 2.2.2.

##### NETLOGON\_VALIDATION\_SAM\_INFO

The NETLOGON\_VALIDATION\_SAM\_INFO structure defines account information retrieved from a [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) upon a successful user logon validation.

All fields of this structure, except the fields detailed following the structure definition, have the same meaning as the identically named fields in the KERB\_VALIDATION\_INFO structure, as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section2.5. Additionally, fields of this structure that are defined as OLD\_LARGE\_INTEGER are 64-bit timestamps equivalent to the identically named fields in the KERB\_VALIDATION\_INFO structure of **FILETIME** type ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.3).

1. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO {
2. OLD\_LARGE\_INTEGER LogonTime;
3. OLD\_LARGE\_INTEGER LogoffTime;
4. OLD\_LARGE\_INTEGER KickOffTime;
5. OLD\_LARGE\_INTEGER PasswordLastSet;
6. OLD\_LARGE\_INTEGER PasswordCanChange;
7. OLD\_LARGE\_INTEGER PasswordMustChange;
8. RPC\_UNICODE\_STRING EffectiveName;
9. RPC\_UNICODE\_STRING FullName;
10. RPC\_UNICODE\_STRING LogonScript;
11. RPC\_UNICODE\_STRING ProfilePath;
12. RPC\_UNICODE\_STRING HomeDirectory;
13. RPC\_UNICODE\_STRING HomeDirectoryDrive;
14. USHORT LogonCount;
15. USHORT BadPasswordCount;
16. ULONG UserId;
17. ULONG PrimaryGroupId;
18. ULONG GroupCount;
19. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
20. ULONG UserFlags;
21. USER\_SESSION\_KEY UserSessionKey;
22. RPC\_UNICODE\_STRING LogonServer;
23. RPC\_UNICODE\_STRING LogonDomainName;
24. PRPC\_SID LogonDomainId;
25. ULONG ExpansionRoom[10];
26. } NETLOGON\_VALIDATION\_SAM\_INFO,
27. \*PNETLOGON\_VALIDATION\_SAM\_INFO;

**LogonServer:**  An **RPC\_UNICODE\_STRING** structure (defined in [MS-DTYP] section 2.3.10) that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the server that populates this structure.

**ExpansionRoom:**  A ten-element array of unsigned 32-bit integers. This member has a function similar to that of dummy fields, as detailed in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046). Each element of the array MUST be zero when sent, and MUST be ignored on receipt.

##### NETLOGON\_VALIDATION\_SAM\_INFO2

The NETLOGON\_VALIDATION\_SAM\_INFO2 structure is an extension to [NETLOGON\_VALIDATION\_SAM\_INFO](#Section_142a277fe16145ac8b95b94bb169b5da), as specified in section 2.2.1.4.11, with support for storing extra [**SIDs**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d).

All fields of this structure, except the fields detailed following the structure definition, have the same meaning as the identically named fields in the KERB\_VALIDATION\_INFO structure as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section 2.5. Additionally, fields of this structure that are defined as OLD\_LARGE\_INTEGER are 64-bit timestamps equivalent to the identically named fields in the KERB\_VALIDATION\_INFO structure of **FILETIME** type ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.3).

1. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO2 {
2. OLD\_LARGE\_INTEGER LogonTime;
3. OLD\_LARGE\_INTEGER LogoffTime;
4. OLD\_LARGE\_INTEGER KickOffTime;
5. OLD\_LARGE\_INTEGER PasswordLastSet;
6. OLD\_LARGE\_INTEGER PasswordCanChange;
7. OLD\_LARGE\_INTEGER PasswordMustChange;
8. RPC\_UNICODE\_STRING EffectiveName;
9. RPC\_UNICODE\_STRING FullName;
10. RPC\_UNICODE\_STRING LogonScript;
11. RPC\_UNICODE\_STRING ProfilePath;
12. RPC\_UNICODE\_STRING HomeDirectory;
13. RPC\_UNICODE\_STRING HomeDirectoryDrive;
14. USHORT LogonCount;
15. USHORT BadPasswordCount;
16. ULONG UserId;
17. ULONG PrimaryGroupId;
18. ULONG GroupCount;
19. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
20. ULONG UserFlags;
21. USER\_SESSION\_KEY UserSessionKey;
22. RPC\_UNICODE\_STRING LogonServer;
23. RPC\_UNICODE\_STRING LogonDomainName;
24. PRPC\_SID LogonDomainId;
25. ULONG ExpansionRoom[10];
26. ULONG SidCount;
27. [size\_is(SidCount)] PNETLOGON\_SID\_AND\_ATTRIBUTES ExtraSids;
28. } NETLOGON\_VALIDATION\_SAM\_INFO2,
29. \*PNETLOGON\_VALIDATION\_SAM\_INFO2;

**LogonServer:**  An **RPC\_UNICODE\_STRING** structure that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the server that populates this structure.

**ExpansionRoom:**  A ten-element array of unsigned 32-bit integers. This member has a function similar to that of dummy fields, as detailed in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046). Each element of the array MUST be zero when sent, and MUST be ignored on receipt.

##### NETLOGON\_VALIDATION\_SAM\_INFO4

The NETLOGON\_VALIDATION\_SAM\_INFO4 structure extends [NETLOGON\_VALIDATION\_SAM\_INFO2](#Section_2a12e28979044ecb9d836732200230c0), as specified in section 2.2.1.4.12, by storing the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e)of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) of the user account and the user [**principal**](#gt_8492780e-99e2-47ba-8553-aedb8de9f9c0).

All fields of this structure, except the fields detailed following the structure definition, have the same meaning as the identically named fields in the KERB\_VALIDATION\_INFO structure, as specified in [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962) section 2.5. Additionally, fields of this structure that are defined as OLD\_LARGE\_INTEGER are 64-bit timestamps equivalent to the identically named fields in the KERB\_VALIDATION\_INFO structure of **FILETIME** type ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.3).

1. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO4 {
2. OLD\_LARGE\_INTEGER LogonTime;
3. OLD\_LARGE\_INTEGER LogoffTime;
4. OLD\_LARGE\_INTEGER KickOffTime;
5. OLD\_LARGE\_INTEGER PasswordLastSet;
6. OLD\_LARGE\_INTEGER PasswordCanChange;
7. OLD\_LARGE\_INTEGER PasswordMustChange;
8. RPC\_UNICODE\_STRING EffectiveName;
9. RPC\_UNICODE\_STRING FullName;
10. RPC\_UNICODE\_STRING LogonScript;
11. RPC\_UNICODE\_STRING ProfilePath;
12. RPC\_UNICODE\_STRING HomeDirectory;
13. RPC\_UNICODE\_STRING HomeDirectoryDrive;
14. unsigned short LogonCount;
15. unsigned short BadPasswordCount;
16. unsigned long UserId;
17. unsigned long PrimaryGroupId;
18. unsigned long GroupCount;
19. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
20. unsigned long UserFlags;
21. USER\_SESSION\_KEY UserSessionKey;
22. RPC\_UNICODE\_STRING LogonServer;
23. RPC\_UNICODE\_STRING LogonDomainName;
24. PRPC\_SID LogonDomainId;
25. unsigned char LMKey[8];
26. ULONG UserAccountControl;
27. ULONG SubAuthStatus;
28. OLD\_LARGE\_INTEGER LastSuccessfulILogon;
29. OLD\_LARGE\_INTEGER LastFailedILogon;
30. ULONG FailedILogonCount;
31. ULONG Reserved4[1];
32. unsigned long SidCount;
33. [size\_is(SidCount)] PNETLOGON\_SID\_AND\_ATTRIBUTES ExtraSids;
34. RPC\_UNICODE\_STRING DnsLogonDomainName;
35. RPC\_UNICODE\_STRING Upn;
36. RPC\_UNICODE\_STRING ExpansionString1;
37. RPC\_UNICODE\_STRING ExpansionString2;
38. RPC\_UNICODE\_STRING ExpansionString3;
39. RPC\_UNICODE\_STRING ExpansionString4;
40. RPC\_UNICODE\_STRING ExpansionString5;
41. RPC\_UNICODE\_STRING ExpansionString6;
42. RPC\_UNICODE\_STRING ExpansionString7;
43. RPC\_UNICODE\_STRING ExpansionString8;
44. RPC\_UNICODE\_STRING ExpansionString9;
45. RPC\_UNICODE\_STRING ExpansionString10;
46. } NETLOGON\_VALIDATION\_SAM\_INFO4,
47. \*PNETLOGON\_VALIDATION\_SAM\_INFO4;

**LogonServer:**  An **RPC\_UNICODE\_STRING** structure that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the server that populates this structure.

**LMKey:**  Contains the first 8 bytes of the LMOWF ([[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) if NTLMV1 is used, or the first 8 bytes of the KXKEY ([MS-NLMP] section 3.4.5.1) if NTLMV2 is used.

**Reserved4:**  An unsigned 32-bit integer. This member is reserved. MUST be zero when sent, and MUST be ignored on receipt.

**DnsLogonDomainName:**  Contains the FQDN (1) of the domain of the user account.

**Upn:**  Contains the [**user principal name (UPN)**](#gt_9d606f55-b798-4def-bf96-97b878bb92c6).

**ExpansionString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. Expansion strings have a function similar to that of dummy fields, as detailed in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**ExpansionString2:**  See description for ExpansionString1.

**ExpansionString3:**  See description for ExpansionString1.

**ExpansionString4:**  See description for ExpansionString1.

**ExpansionString5:**  See description for ExpansionString1.

**ExpansionString6:**  See description for ExpansionString1.

**ExpansionString7:**  See description for ExpansionString1.

**ExpansionString8:**  See description for ExpansionString1.

**ExpansionString9:**  See description for ExpansionString1.

**ExpansionString10:**  See description for ExpansionString1.

##### NETLOGON\_VALIDATION

The NETLOGON\_VALIDATION union defines a union of all types of user validation information values.

1. typedef
2. [switch\_type(enum \_NETLOGON\_VALIDATION\_INFO\_CLASS)]
3. union \_NETLOGON\_VALIDATION {
4. [case(NetlogonValidationSamInfo)]
5. PNETLOGON\_VALIDATION\_SAM\_INFO ValidationSam;
6. [case(NetlogonValidationSamInfo2)]
7. PNETLOGON\_VALIDATION\_SAM\_INFO2 ValidationSam2;
8. [case(NetlogonValidationGenericInfo2)]
9. PNETLOGON\_VALIDATION\_GENERIC\_INFO2 ValidationGeneric2;
10. [case(NetlogonValidationSamInfo4)]
11. PNETLOGON\_VALIDATION\_SAM\_INFO4 ValidationSam4;
12. [default]  ;
13. } NETLOGON\_VALIDATION,
14. \*PNETLOGON\_VALIDATION;

**ValidationSam:**  This field is selected when the validation information type is **NetlogonValidationSamInfo**. The selected data type is [NETLOGON\_VALIDATION\_SAM\_INFO](#Section_142a277fe16145ac8b95b94bb169b5da), as specified in section 2.2.1.4.11.

**ValidationSam2:**  This field is selected when the validation information type is **NetlogonValidationSamInfo2**. The selected data type is [NETLOGON\_VALIDATION\_SAM\_INFO2](#Section_2a12e28979044ecb9d836732200230c0), as specified in section 2.2.1.4.12.

**ValidationGeneric2:**  This field is selected when the validation information type is **NetlogonValidationGenericInfo2**. The selected data type is [NETLOGON\_VALIDATION\_GENERIC\_INFO2](#Section_e89f8f5b098541a0b1101ae0ea2bd183), as specified in section 2.2.1.4.8.

**ValidationSam4:**  This field is selected when the validation information type is **NetlogonValidationSamInfo4**. The selected data type is [NETLOGON\_VALIDATION\_SAM\_INFO4](#Section_bccfdba90c38485eb751d4de1935781d), as specified in section 2.2.1.4.13.

##### NETLOGON\_LOGON\_IDENTITY\_INFO

The NETLOGON\_LOGON\_IDENTITY\_INFO structure defines a logon identity within a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. typedef struct \_NETLOGON\_LOGON\_IDENTITY\_INFO {
2. RPC\_UNICODE\_STRING LogonDomainName;
3. ULONG ParameterControl;
4. OLD\_LARGE\_INTEGER Reserved;
5. RPC\_UNICODE\_STRING UserName;
6. RPC\_UNICODE\_STRING Workstation;
7. } NETLOGON\_LOGON\_IDENTITY\_INFO,
8. \*PNETLOGON\_LOGON\_IDENTITY\_INFO;

**LogonDomainName:**  Contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the domain of the account.

**ParameterControl:**  A set of bit flags that contain information pertaining to the logon validation processing. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| X | W | V | U | T | S | R | Q | 0 | 0 | 0 | P | 0 | 0 | 0 | O | 0 | N | M | L | K | J | I | H | G | F | E | D | C | B | A | 0 |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Clear text passwords can be transmitted for this logon identity. |
| B | Update the logon statistics for this account upon successful logon. |
| C | Return the user parameter list for this account upon successful logon. |
| D | Do not attempt to log this account on as a guest upon logon failure. |
| E | Allow this account to log on with the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) account. |
| F | Return the password expiration date and time upon successful logon. |
| G | Send a [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) upon logon request. |
| H | Attempt logon as a guest for this account only. |
| I | Return the profile path upon successful logon. |
| J | Attempt logon to the specified domain only. |
| K | Allow this account to log on with the computer account. |
| L | Disable allowing fallback to guest account for this account. |
| M | Force the logon of this account as a guest if the password is incorrect. |
| N | This account has supplied a clear text password. |
| O | Allow NTLMv1 authentication ([[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)) when only NTLMv2 ([[NTLM]](https://go.microsoft.com/fwlink/?LinkId=90235)) is allowed. |
| P | Use [**sub-authentication**](#gt_704fc38e-bf60-44b9-adbf-4b842d6141ed) ([[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 3.1.5.2.1). |
| Q - X | Encode the [**sub-authentication package**](#gt_b1331d67-e2ca-45e1-af31-50f52659a0c2) identifier. Bits Q–X are used to encode the integer value of the sub-authentication package identifier (this is in little-endian order). |

**Reserved:**  MUST be set to zero when sent and MUST be ignored on receipt.

**UserName:**  Contains the name of the user.

**Workstation:**  Contains the NetBIOS name of the workstation from which the user is logging on.

##### NETLOGON\_LOGON\_INFO\_CLASS

The NETLOGON\_LOGON\_INFO\_CLASS enumeration SHOULD[<44>](#Appendix_A_44" \o "Product behavior note 44) identify a particular type of logon information block.

1. typedef enum \_NETLOGON\_LOGON\_INFO\_CLASS
2. {
3. NetlogonInteractiveInformation = 1,
4. NetlogonNetworkInformation = 2,
5. NetlogonServiceInformation = 3,
6. NetlogonGenericInformation = 4,
7. NetlogonInteractiveTransitiveInformation = 5,
8. NetlogonNetworkTransitiveInformation = 6,
9. NetlogonServiceTransitiveInformation = 7
10. } NETLOGON\_LOGON\_INFO\_CLASS;

**NetlogonInteractiveInformation:** Logon information pertains to an interactive account logon. Interactive account logon requires a user to physically input [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) to the client that are then authenticated by the [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**NetlogonNetworkInformation:** Logon information pertains to a network account logon. [**Network logon**](#gt_c020fc9f-456f-4fd0-8e25-001ef6b8acf2) is transparent to the user. The user has already input his or her credentials during [**interactive logon**](#gt_9360639b-135c-46dc-9f9e-85728008146f) and has been authenticated by the server or DC. These credentials are used again to log the user onto another network resource without prompting the user for his or her credentials.

**NetlogonServiceInformation:** Logon information pertains to a service account logon. A service account acts as a non-privileged user on the local computer and presents anonymous credentials to any remote server.

**NetlogonGenericInformation:** Logon information pertains to a generic account logon. This type of account logon is for generic pass-through authentication, as specified in section [3.2.4.1](#Section_fe2775d4a3e24971a2558eef8dd27a27), that enables servers to forward NTLM and Digest authentication credentials to a DC for authorization.

**NetlogonInteractiveTransitiveInformation:** Logon information pertains to a transitive interactive account logon and can be passed through [**transitive trust**](#gt_1c9fbb3f-ba87-419f-bd0c-39f73cee86f7) links.

**NetlogonNetworkTransitiveInformation:** Logon information pertains to a transitive network account logon and can be passed through transitive trust links.

**NetlogonServiceTransitiveInformation:** Logon information pertains to a transitive service account logon and can be passed through transitive trust links.

##### NETLOGON\_VALIDATION\_INFO\_CLASS

The NETLOGON\_VALIDATION\_INFO\_CLASS enumeration SHOULD[<45>](#Appendix_A_45" \o "Product behavior note 45) select the type of logon information block being used.

1. typedef enum \_NETLOGON\_VALIDATION\_INFO\_CLASS
2. {
3. NetlogonValidationUasInfo = 1,
4. NetlogonValidationSamInfo = 2,
5. NetlogonValidationSamInfo2 = 3,
6. NetlogonValidationGenericInfo = 4,
7. NetlogonValidationGenericInfo2 = 5,
8. NetlogonValidationSamInfo4 = 6
9. } NETLOGON\_VALIDATION\_INFO\_CLASS;

**NetlogonValidationUasInfo:** Associated structure is [NETLOGON\_VALIDATION\_UAS\_INFO (section 2.2.1.8.1)](#Section_7bd204f6aba3464cb02855e49f7999a0).[<46>](#Appendix_A_46" \o "Product behavior note 46)

**NetlogonValidationSamInfo:** Associated structure is [NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11)](#Section_142a277fe16145ac8b95b94bb169b5da).

**NetlogonValidationSamInfo2:** Associated structure is [NETLOGON\_VALIDATION\_SAM\_INFO2 (section 2.2.1.4.12)](#Section_2a12e28979044ecb9d836732200230c0).

**NetlogonValidationGenericInfo:** Associated structure is [NETLOGON\_VALIDATION\_GENERIC\_INFO2 (section 2.2.1.4.8)](#Section_e89f8f5b098541a0b1101ae0ea2bd183).

**NetlogonValidationGenericInfo2:** Associated structure is NETLOGON\_VALIDATION\_GENERIC\_INFO2 (section 2.2.1.4.8).

**NetlogonValidationSamInfo4:** Associated structure is [NETLOGON\_VALIDATION\_SAM\_INFO4 (section 2.2.1.4.13)](#Section_bccfdba90c38485eb751d4de1935781d).

##### NETLOGON Specific Access Masks

**Access Rights**: The access rights defined by this protocol are specified by the bit settings in the following table:

| Name | Value | Informative Summary |
| --- | --- | --- |
| NETLOGON\_UAS\_LOGON\_ACCESS | 0x0001 | Obsolete (LAN Manager). |
| NETLOGON\_UAS\_LOGOFF\_ACCESS | 0x0002 | Obsolete (LAN Manager). |
| NETLOGON\_CONTROL\_ACCESS | 0x0004 | Granted to [**security principals**](#gt_f3ef2572-95cf-4c5c-b3c9-551fd648f409) that are system operators, account operators, administrators, or components of the operating system. |
| NETLOGON\_QUERY\_ACCESS | 0x0008 | Granted to all security principals. |
| NETLOGON\_SERVICE\_ACCESS | 0x0010 | Granted to all security principals that are administrators or components of the operating system. |
| NETLOGON\_FTINFO\_ACCESS | 0x0020 | Granted to all security principals that are authenticated users. |
| NETLOGON\_WKSTA\_RPC\_ACCESS | 0x0040 | Granted to all security principals that are local users or administrators. |

#### Account Database Replication Structures

Structures and enumerated types in this group are used for account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) replication as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7). These structures are relevant only for server-to-server communication, and are obsolete.

##### NETLOGON\_DB\_CHANGE (Announcement) Message

The following is the format of the payload of a [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) message used in Netlogon replication, as specified in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761). The message is used to indicate that one or more changes have taken place in the account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15), and carries an indication of the changes from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to the BDC. Because it is sent in the open, this is a hint, and the BDC must connect to the PDC over a reliable transport and secure connection to obtain the actual change.

The DBChangeInfo field represents information about a state of one of the databases ([**security account manager (SAM) built-in database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b), [**Security Account Manager (SAM)**](#gt_0b53d5bb-74ab-4705-8657-c22d32781103), or [**Local Security Authority**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b)). The number of DBChangeInfo fields is specified by the DBCount field. The format of the DBChangeInfo field is described below.

The fields in the above diagram are in little-endian format and have the following meanings:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| MessageType | | | | | | | | | | | | | | | | LowSerialNumber | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | DateAndTime | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | Pulse | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | Random | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | PrimaryDCName (variable) | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DomainName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UnicodePrimaryDCName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| UnicodeDomainName (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DBCount | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DBChangeInfo (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DomainSidSize | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DomainSid (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MessageFormatVersion | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| MessageToken | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**MessageType (2 bytes):** A two-byte field identifying the message. MUST be set to 0x000A.

**LowSerialNumber (4 bytes):** The low DWORD part of the 64-bit [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) of the SAM database.

**DateAndTime (4 bytes):** An unsigned 32-bit value representing the time stamp for the SAM database creation time. This MUST be expressed as the number of seconds elapsed since midnight of January 1, 1970.

**Pulse (4 bytes):** An unsigned 32-bit value that specifies the message interval in seconds between change announcements sent to the BDCs.

**Random (4 bytes):** An unsigned 32-bit value that indicates the number of seconds the recipient of the message SHOULD[<47>](#Appendix_A_47" \o "Product behavior note 47) wait before contacting the sender.

**PrimaryDCName (variable):** The null-terminated name of the PDC sending the message. MUST be encoded in the [**original equipment manufacturer (OEM) character set**](#gt_3240e34e-920e-40ac-a672-342ac34a5e22).

**DomainName (variable):** The null-terminated [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) encoded in the OEM character set. The domain name is padded to a multiple of 2 bytes for alignment reasons.

**UnicodePrimaryDCName (variable):** The null-terminated name of the PDC sending the message. MUST be encoded in the [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) character set.

**UnicodeDomainName (variable):** The null-terminated domain name. MUST be encoded in the Unicode character set.

**DBCount (4 bytes):** An unsigned 32-bit value representing the number of DBChangeInfo fields in the message.

**DBChangeInfo (variable):** A set of **DBChangeInfo** messages, specified below, that indicate the changes that are pending replication. There are **DBCount** entries in this set.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| DBIndex | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LargeSerialNumber | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DateAndTime | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**DBIndex (4 bytes):** A 32-bit value that identifies the database as follows:

| Value | Meaning |
| --- | --- |
| 0x00000000 | Indicates the SAM database. |
| 0x00000001 | Indicates the SAM built-in database. |
| 0x00000002 | Indicates the LSA database. |

**LargeSerialNumber (8 bytes):** A 64-bit value that contains the database serial number for the database identified by the **DBIndex** field.

**DateAndTime (8 bytes):** The time in UTC of the database creation expressed as an 8-byte value in the TIME format in a **FILETIME** structure, as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) Appendix A (section 6).

In what follows, the above message is referred to as the announcement message.

**DomainSidSize (4 bytes):** An unsigned 32-bit value specifying the size in bytes of the DomainSid field.

**DomainSid (variable):** The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**MessageFormatVersion (4 bytes):** An unsigned 32-bit value containing the version of the message format. MUST be set to 0x00000001.

**MessageToken (4 bytes):** An unsigned 32-bit field identifying the message. MUST be set to 0xFFFFFFFF.

##### NLPR\_QUOTA\_LIMITS

The NLPR\_QUOTA\_LIMITS structure defines a set of system resources that are available to a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) user.

1. typedef struct \_NLPR\_QUOTA\_LIMITS {
2. ULONG PagedPoolLimit;
3. ULONG NonPagedPoolLimit;
4. ULONG MinimumWorkingSetSize;
5. ULONG MaximumWorkingSetSize;
6. ULONG PagefileLimit;
7. OLD\_LARGE\_INTEGER Reserved;
8. } NLPR\_QUOTA\_LIMITS,
9. \*PNLPR\_QUOTA\_LIMITS;

**PagedPoolLimit:**   Specifies the number of bytes of paged pool memory assigned to the user. The paged pool is an area of system memory (physical memory used by the operating system) for objects that can be written to disk when they are not being used.

**NonPagedPoolLimit:**  Specifies the number of bytes of nonpaged pool memory assigned to the user. The nonpaged pool is an area of system memory for objects that cannot be written to disk but MUST remain in physical memory as long as they are allocated.

**MinimumWorkingSetSize:**  Specifies the minimum set size assigned to the user. The working set of a process is the set of memory pages currently visible to the process in physical RAM memory. These pages are present in memory when the application is running and available for an application to use without triggering a page fault.

**MaximumWorkingSetSize:**  Specifies the maximum set size assigned to the user.

**PagefileLimit:**  Specifies the maximum size, in bytes, of the paging file, which is a reserved space on disk that backs up committed physical memory on the computer.

**Reserved:**  SHOULD be set to zero and MUST be ignored on receipt.

##### NETLOGON\_DELTA\_ACCOUNTS

The NETLOGON\_DELTA\_ACCOUNTS structure contains the settings and [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940) for a [**Local Security Authority (LSA)**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) account. This structure is used for replicating the LSA account data from the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a [**backup domain controller (BDC)**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3).

1. typedef struct \_NETLOGON\_DELTA\_ACCOUNTS {
2. ULONG PrivilegeEntries;
3. ULONG PrivilegeControl;
4. [size\_is(PrivilegeEntries)] ULONG\* PrivilegeAttributes;
5. [size\_is(PrivilegeEntries)] PRPC\_UNICODE\_STRING PrivilegeNames;
6. NLPR\_QUOTA\_LIMITS QuotaLimits;
7. ULONG SystemAccessFlags;
8. SECURITY\_INFORMATION SecurityInformation;
9. ULONG SecuritySize;
10. [size\_is(SecuritySize)] UCHAR\* SecurityDescriptor;
11. RPC\_UNICODE\_STRING DummyString1;
12. RPC\_UNICODE\_STRING DummyString2;
13. RPC\_UNICODE\_STRING DummyString3;
14. RPC\_UNICODE\_STRING DummyString4;
15. ULONG DummyLong1;
16. ULONG DummyLong2;
17. ULONG DummyLong3;
18. ULONG DummyLong4;
19. } NETLOGON\_DELTA\_ACCOUNTS,
20. \*PNETLOGON\_DELTA\_ACCOUNTS;

**PrivilegeEntries:**  The number of privileges associated with the LSA account.

**PrivilegeControl:**  A bit flag describing the properties of the account privileges. A flag is TRUE (or set) if its value is equal to 1. PrivilegeControl MAY be the following value.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | All of the specified privileges MUST be held by the process that is requesting access. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**PrivilegeAttributes:**  Pointer to an array of unsigned 32-bit values that contain a set of bit flags describing each privilege's attributes. An attribute is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Privilege is enabled by default. |
| B | Privilege is enabled. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**PrivilegeNames:**  A pointer to an array of privilege names represented as RPC\_UNICODE\_STRING structures. See [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10 for a specification of the RPC\_UNICODE\_STRING structure. The names of the privileges are implementation-specific.

**QuotaLimits:**  An NLPR\_QUOTA\_LIMITS structure that describes the account's current quota settings. For more details about the NLPR\_QUOTA\_LIMITS structure, see section [2.2.1.5.2](#Section_55d7ea86c4cc4a5e8414426673cb77d1).

**SystemAccessFlags:**  A set of the following bit flags that specify the ways in which the account is permitted to access the system as detailed in POLICY\_MODE\_INTERACTIVE, POLICY\_MODE\_NETWORK, POLICY\_MODE\_BATCH, POLICY\_MODE\_SERVICE, and POLICY\_MODE\_PROXY of [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc). See [MS-LSAD] for the specification of these bit values and allowed combinations.

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [MS-DTYP] section 2.4.7, that specifies portions of a security descriptor about the [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that describes the security settings for the account object.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

##### NETLOGON\_DELTA\_ALIAS

The NETLOGON\_DELTA\_ALIAS structure contains information about a SAM [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd). This structure is used to replicate the SAM alias data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC.

1. typedef struct \_NETLOGON\_DELTA\_ALIAS {
2. RPC\_UNICODE\_STRING Name;
3. ULONG RelativeId;
4. SECURITY\_INFORMATION SecurityInformation;
5. ULONG SecuritySize;
6. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
7. RPC\_UNICODE\_STRING Comment;
8. RPC\_UNICODE\_STRING DummyString2;
9. RPC\_UNICODE\_STRING DummyString3;
10. RPC\_UNICODE\_STRING DummyString4;
11. ULONG DummyLong1;
12. ULONG DummyLong2;
13. ULONG DummyLong3;
14. ULONG DummyLong4;
15. } NETLOGON\_DELTA\_ALIAS,
16. \*PNETLOGON\_DELTA\_ALIAS;

**Name:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the alias name.

**RelativeId:**  The [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) for the alias.

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [MS-DTYP] section 2.4.7, that contains security settings for the alias.

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that describes the security information for the alias object.

**Comment:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, that contains the administrative comment string for the alias.

**DummyString2:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString3:**  See description for DummyString2.

**DummyString4:**  See description for DummyString2.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  See DummyLong1.

**DummyLong3:**  See DummyLong1.

**DummyLong4:**  See DummyLong1.

##### NLPR\_SID\_INFORMATION

The NLPR\_SID\_INFORMATION structure is used to form a wrapper for a [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d); it is used to transmit a SID during certain replication operations. See section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761) for details.

1. typedef struct \_NLPR\_SID\_INFORMATION {
2. PRPC\_SID SidPointer;
3. } NLPR\_SID\_INFORMATION,
4. \*PNLPR\_SID\_INFORMATION;

**SidPointer:**  A pointer to a SID structure.

##### NLPR\_SID\_ARRAY

The NLPR\_SID\_ARRAY structure defines an array of pointers to [**security identifier**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) structures.

1. typedef struct \_NLPR\_SID\_ARRAY {
2. ULONG Count;
3. [size\_is(Count)] PNLPR\_SID\_INFORMATION Sids;
4. } NLPR\_SID\_ARRAY,
5. \*PNLPR\_SID\_ARRAY;

**Count:**  The number of pointers in the **Sids** array.

**Sids:**  An array of NLPR\_SID\_INFORMATION structures, as specified in section [2.2.1.5.5](#Section_e936e7db27cb40ddacf7eec6ac0e9ed5), each of which is a pointer to a SID.

##### NETLOGON\_DELTA\_ALIAS\_MEMBER

The NETLOGON\_DELTA\_ALIAS\_MEMBER structure contains all the members of a SAM [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd). This structure is used for replicating the SAM alias data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

1. typedef struct \_NETLOGON\_DELTA\_ALIAS\_MEMBER {
2. NLPR\_SID\_ARRAY Members;
3. ULONG DummyLong1;
4. ULONG DummyLong2;
5. ULONG DummyLong3;
6. ULONG DummyLong4;
7. } NETLOGON\_DELTA\_ALIAS\_MEMBER,
8. \*PNETLOGON\_DELTA\_ALIAS\_MEMBER;

**Members:**  An NLPR\_SID\_ARRAY structure, as specified in section [2.2.1.5.6](#Section_d89f92c6bc7c4af3a96d835e9ab03ca0), that contains an array of [**SIDs**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) for each member of the alias.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

##### NETLOGON\_DELTA\_DELETE\_GROUP

The NETLOGON\_DELTA\_DELETE\_GROUP structure contains information about a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) to be deleted in the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). This structure is used for replicating the SAM group data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

1. typedef struct \_NETLOGON\_DELTA\_DELETE\_GROUP {
2. [string] wchar\_t\* AccountName;
3. RPC\_UNICODE\_STRING DummyString1;
4. RPC\_UNICODE\_STRING DummyString2;
5. RPC\_UNICODE\_STRING DummyString3;
6. RPC\_UNICODE\_STRING DummyString4;
7. ULONG DummyLong1;
8. ULONG DummyLong2;
9. ULONG DummyLong3;
10. ULONG DummyLong4;
11. } NETLOGON\_DELTA\_DELETE\_GROUP,
12. \*PNETLOGON\_DELTA\_DELETE\_GROUP;

**AccountName:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the group to delete.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is specified in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_DELTA\_DELETE\_USER

The NETLOGON\_DELTA\_DELETE\_USER structure contains information about a user account to be deleted in the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15).

1. typedef struct \_NETLOGON\_DELTA\_DELETE\_USER {
2. [string] wchar\_t\* AccountName;
3. RPC\_UNICODE\_STRING DummyString1;
4. RPC\_UNICODE\_STRING DummyString2;
5. RPC\_UNICODE\_STRING DummyString3;
6. RPC\_UNICODE\_STRING DummyString4;
7. ULONG DummyLong1;
8. ULONG DummyLong2;
9. ULONG DummyLong3;
10. ULONG DummyLong4;
11. } NETLOGON\_DELTA\_DELETE\_USER,
12. \*PNETLOGON\_DELTA\_DELETE\_USER;

**AccountName:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the user to delete.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is specified in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_DELTA\_DOMAIN

The NETLOGON\_DELTA\_DOMAIN structure contains information about a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). Most of the fields in this structure are obtained by querying the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). This structure is used to replicate the domain data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

All fields of this structure, except the fields detailed following the structure definition, have the same meaning as the identically named fields in the Domain Fields section ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.4.1).

1. typedef struct \_NETLOGON\_DELTA\_DOMAIN {
2. RPC\_UNICODE\_STRING DomainName;
3. RPC\_UNICODE\_STRING OemInformation;
4. OLD\_LARGE\_INTEGER ForceLogoff;
5. USHORT MinPasswordLength;
6. USHORT PasswordHistoryLength;
7. OLD\_LARGE\_INTEGER MaxPasswordAge;
8. OLD\_LARGE\_INTEGER MinPasswordAge;
9. OLD\_LARGE\_INTEGER DomainModifiedCount;
10. OLD\_LARGE\_INTEGER DomainCreationTime;
11. SECURITY\_INFORMATION SecurityInformation;
12. ULONG SecuritySize;
13. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
14. RPC\_UNICODE\_STRING DomainLockoutInformation;
15. RPC\_UNICODE\_STRING DummyString2;
16. RPC\_UNICODE\_STRING DummyString3;
17. RPC\_UNICODE\_STRING DummyString4;
18. ULONG PasswordProperties;
19. ULONG DummyLong2;
20. ULONG DummyLong3;
21. ULONG DummyLong4;
22. } NETLOGON\_DELTA\_DOMAIN,
23. \*PNETLOGON\_DELTA\_DOMAIN;

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.7, that specifies portions of a security descriptor about the domain.

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that contains the security settings for the domain object.

**DomainLockoutInformation:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, that contains the domain lockout information detailed in [MS-SAMR]. The **Buffer** field points to the SAMPR\_DOMAIN\_LOCKOUT\_INFORMATION structure, as specified in [MS-SAMR] section 2.2.4.15, and the **Length** and **MaximumLength** fields are set to the size in bytes of the SAMPR\_DOMAIN\_LOCKOUT\_INFORMATION structure pointed to by the **Buffer** field.

**DummyString2:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is specified in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString3:**  See description for DummyString2.

**DummyString4:**  See description for DummyString2.

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong3:**  See description for DummyLong2.

**DummyLong4:**  See description for DummyLong2.

##### NETLOGON\_DELTA\_ENUM

The NETLOGON\_DELTA\_ENUM structure defines a common structure that encapsulates all possible types of [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) changes. Database changes, in the context of Netlogon, are called [**deltas**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e).

1. typedef struct \_NETLOGON\_DELTA\_ENUM {
2. NETLOGON\_DELTA\_TYPE DeltaType;
3. [switch\_is(DeltaType)] NETLOGON\_DELTA\_ID\_UNION DeltaID;
4. [switch\_is(DeltaType)] NETLOGON\_DELTA\_UNION DeltaUnion;
5. } NETLOGON\_DELTA\_ENUM,
6. \*PNETLOGON\_DELTA\_ENUM;

**DeltaType:**  One of the values from the NETLOGON\_DELTA\_TYPE enumeration, as specified in section [2.2.1.5.28](#Section_f8a8cd32426d45f1be45e0dc5c1c1359).

**DeltaID:**  One of the [NETLOGON\_DELTA\_ID\_UNION](#Section_797e1033d40b400ba71a522f820bac33) types selected based on the value of the **DeltaType** field.

**DeltaUnion:**  One of the [NETLOGON\_DELTA\_UNION](#Section_3d07c30c9f0e4aa3a9d08fc348fd1fe1) types selected based on the value of the **DeltaType** field.

##### NETLOGON\_DELTA\_ENUM\_ARRAY

The NETLOGON\_DELTA\_ENUM\_ARRAY structure defines an array of [**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e) objects.

1. typedef struct \_NETLOGON\_DELTA\_ENUM\_ARRAY {
2. DWORD CountReturned;
3. [size\_is(CountReturned)] PNETLOGON\_DELTA\_ENUM Deltas;
4. } NETLOGON\_DELTA\_ENUM\_ARRAY,
5. \*PNETLOGON\_DELTA\_ENUM\_ARRAY;

**CountReturned:**  The number of elements in the Deltas field.

**Deltas:**  An array of NETLOGON\_DELTA\_ENUM structures, as specified in section [2.2.1.5.11](#Section_20e5863c014240f6a914f352a9d66047).

##### NETLOGON\_DELTA\_GROUP

The NETLOGON\_DELTA\_GROUP structure contains information about a SAM [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) account. This structure is used for replicating the group data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

1. typedef struct \_NETLOGON\_DELTA\_GROUP {
2. RPC\_UNICODE\_STRING Name;
3. ULONG RelativeId;
4. ULONG Attributes;
5. RPC\_UNICODE\_STRING AdminComment;
6. SECURITY\_INFORMATION SecurityInformation;
7. ULONG SecuritySize;
8. [size\_is(SecuritySize)] UCHAR\* SecurityDescriptor;
9. RPC\_UNICODE\_STRING DummyString1;
10. RPC\_UNICODE\_STRING DummyString2;
11. RPC\_UNICODE\_STRING DummyString3;
12. RPC\_UNICODE\_STRING DummyString4;
13. ULONG DummyLong1;
14. ULONG DummyLong2;
15. ULONG DummyLong3;
16. ULONG DummyLong4;
17. } NETLOGON\_DELTA\_GROUP,
18. \*PNETLOGON\_DELTA\_GROUP;

**Name:**  A RPC\_UNICODE\_STRING structure that contains the group name.

**RelativeId:**  The [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) for the group.

**Attributes:**  A set of bit flags that describe attributes of the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d). An attribute is true (or set) if its value is equal to 1. The value is constructed from one or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | The SID cannot have the **SE\_GROUP\_ENABLED** attribute removed. Corresponds to the SID attribute **SE\_GROUP\_MANDATORY**. This attribute prevents the user from disabling the group. Disabling a group causes the group to be ignored by access validation routines. For more information, see [[SIDATT]](https://go.microsoft.com/fwlink/?LinkId=90515). |
| B | The SID is enabled by default (as opposed to being enabled by an application). Corresponds to the SID attribute **SE\_GROUP\_ENABLED\_BY\_DEFAULT**. For more information, see [SIDATT]. |
| C | The SID is enabled for access checks. Corresponds to the SID attribute **SE\_GROUP\_ENABLED**. For more information, see [SIDATT]. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**AdminComment:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains an administrative comment for the group.

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [MS-DTYP] section 2.4.7, that specifies portions of a security descriptor about the group.

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that contains the security settings of the group object.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2** See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NLPR\_LOGON\_HOURS

The NLPR\_LOGON\_HOURS structure contains the logon policy information that specifies when a user account is permitted to authenticate.

1. typedef struct \_NLPR\_LOGON\_HOURS {
2. USHORT UnitsPerWeek;
3. [size\_is(1260), length\_is((UnitsPerWeek + 7)/8)]
4. UCHAR \* LogonHours;
5. } NLPR\_LOGON\_HOURS,
6. \*PNLPR\_LOGON\_HOURS;

The fields in this structure have the same meanings as identically named fields of the SAMPR\_LOGON\_HOURS structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.7.5.

##### NLPR\_USER\_PRIVATE\_INFO

The NLPR\_USER\_PRIVATE\_INFO structure defines a data buffer that is optionally encrypted with the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d), as detailed in this section. The structure is used to carry user account passwords as follows.

1. typedef struct \_NLPR\_USER\_PRIVATE\_INFO {
2. UCHAR SensitiveData;
3. ULONG DataLength;
4. [size\_is(DataLength)] UCHAR \* Data;
5. } NLPR\_USER\_PRIVATE\_INFO,
6. \*PNLPR\_USER\_PRIVATE\_INFO;

**SensitiveData:**  Is either TRUE (0x01) or FALSE (0x00). The **SensitiveData** field indicates whether the data is encrypted as follows. If this field is set to 0x00, then the data is not encrypted. If the field is set to 0x01, the data pointed to by the **Data** field is encrypted with the session key used on the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) between the client and the server exchanging this data structure to the client. The encryption algorithm is [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) if the flag C is set in the negotiated flags between the client and the server, as specified in section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed); otherwise the encryption algorithm is DES.

**DataLength:** The size, in bytes, of the **Data** field.

**Data:**  A pointer to a buffer with a size of **DataLength**. If the **SensitiveData** field is set to TRUE, this data is encrypted as described in the description of the **SensitiveData** field. The buffer content prior to encryption (if any) is shown in the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| DataType | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmLength | | | | | | | | | | | | | | | | LmMaximumLength | | | | | | | | | | | | | | | |
| Unused1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHash[0..3] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHash[4..7] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHash[8..11] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHash[12..15] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtLength | | | | | | | | | | | | | | | | NtMaximumLength | | | | | | | | | | | | | | | |
| Unused2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHash[0..3] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHash[4..7] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHash[8..11] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHash[12..15] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHistoryLength | | | | | | | | | | | | | | | | LmHistoryMaximumLength | | | | | | | | | | | | | | | |
| Unused3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHistoryLength | | | | | | | | | | | | | | | | NtHistoryMaximumLength | | | | | | | | | | | | | | | |
| Unused4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NtHistoryArray (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LmHistoryArray (variable) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ... | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**DataType:** An unsigned integer. This value MUST be 0x00000002.

**LmLength:** An unsigned (short) integer. This value MUST be either 0x0010 or 0x0000. If 0x0010, the **LmHash** field contains the LM hash of the user password (specified in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)). If 0x0000, the value of the **LmHash** field is undefined and MUST be ignored upon receipt.

**LmMaximumLength:** This value MUST be the same value as **LmLength**.

**Unused1:** This value MUST be zero and ignored on receipt.

**LmHash:** The encrypted ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.11.1) LM OWF ([MS-NLMP] section 3.3) of the user password. The 16-byte [**encryption key**](#gt_fbdcfa70-e954-4dbd-bafa-0f9c4bcf90dd) is created by concatenating four times the relative ID (from the given user's [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d)).

**NtLength:** An unsigned (short) integer. This value MUST be either 0x0010 or 0x0000. If 0x0010, the **NtHash** field contains the NT hash of the user password (specified in [MS-NLMP]). If 0x0000, the value of the **NtHash** field is undefined and MUST be ignored upon receipt.

**NtMaximumLength:** This value MUST be the same value as **NtLength**.

**Unused2:** This value SHOULD be zero and ignored on receipt.

**NtHash:** The encrypted ([MS-SAMR] section 2.2.11.1) NT OWF ([MS-NLMP] section 3.3) of the user password. The 16-byte encryption key is created by concatenating four times the relative ID (from the given user's SID).

**LmHistoryLength:** An unsigned (short) integer. This value is the length, in bytes, of the **LmHistoryArray** field.

**LmHistoryMaximumLength:** This value MUST be the same value as **LmHistoryLength**.

**Unused3:** This value SHOULD be zero and ignored on receipt.

**NtHistoryLength**: An unsigned (short) integer. This value is the length, in bytes, of the **NtHistoryArray** field.

**NtHistoryMaximumLength:** This value MUST be the same value as **NtHistoryLength**.

**Unused4**: This value SHOULD be zero and ignored on receipt.

**NtHistoryArray:** An array of NT hash values of user passwords for the given user. The array is ordered so that the first element is the hash of the current password and the last element is the hash of the oldest password.

**Note**  The number of elements in the array is the value of the **NtHistoryLength** field divided by 0x0010.

**LmHistoryArray:** An array of LM hash values of user passwords for the given user. The array is ordered so that the first element is the hash of the current password and the last element is the hash of the oldest password.

**Note**  The number of elements in the array is the value of the **LmHistoryLength** field divided by 0x0010.

##### NETLOGON\_DELTA\_USER

The NETLOGON\_DELTA\_USER structure contains information about a SAM user account. This structure is used for replicating the user account data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

All fields of this structure, except the fields detailed following the structure definition, have the same meanings as the identically named fields in the Common User Fields, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.7.1 and the SAMPR\_USER\_INTERNAL1\_INFORMATION structure fields, as specified in [MS-SAMR] section 2.2.7.23.

1. typedef struct \_NETLOGON\_DELTA\_USER {
2. RPC\_UNICODE\_STRING UserName;
3. RPC\_UNICODE\_STRING FullName;
4. ULONG UserId;
5. ULONG PrimaryGroupId;
6. RPC\_UNICODE\_STRING HomeDirectory;
7. RPC\_UNICODE\_STRING HomeDirectoryDrive;
8. RPC\_UNICODE\_STRING ScriptPath;
9. RPC\_UNICODE\_STRING AdminComment;
10. RPC\_UNICODE\_STRING WorkStations;
11. OLD\_LARGE\_INTEGER LastLogon;
12. OLD\_LARGE\_INTEGER LastLogoff;
13. NLPR\_LOGON\_HOURS LogonHours;
14. USHORT BadPasswordCount;
15. USHORT LogonCount;
16. OLD\_LARGE\_INTEGER PasswordLastSet;
17. OLD\_LARGE\_INTEGER AccountExpires;
18. ULONG UserAccountControl;
19. ENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNtOwfPassword;
20. ENCRYPTED\_LM\_OWF\_PASSWORD EncryptedLmOwfPassword;
21. UCHAR NtPasswordPresent;
22. UCHAR LmPasswordPresent;
23. UCHAR PasswordExpired;
24. RPC\_UNICODE\_STRING UserComment;
25. RPC\_UNICODE\_STRING Parameters;
26. USHORT CountryCode;
27. USHORT CodePage;
28. NLPR\_USER\_PRIVATE\_INFO PrivateData;
29. SECURITY\_INFORMATION SecurityInformation;
30. ULONG SecuritySize;
31. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
32. RPC\_UNICODE\_STRING ProfilePath;
33. RPC\_UNICODE\_STRING DummyString2;
34. RPC\_UNICODE\_STRING DummyString3;
35. RPC\_UNICODE\_STRING DummyString4;
36. ULONG DummyLong1;
37. ULONG DummyLong2;
38. ULONG DummyLong3;
39. ULONG DummyLong4;
40. } NETLOGON\_DELTA\_USER,
41. \*PNETLOGON\_DELTA\_USER;

**PrivateData:**  An NLPR\_USER\_PRIVATE\_INFO structure, as specified in section [2.2.1.5.15](#Section_1333d2308d174c16a09d0b7c785d591a), containing the **PrivateData** field of the SAMPR\_USER\_INFORMATION structure, as specified in [MS-SAMR] section 2.2.7.6.

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.7, that specifies portions of a security descriptor about the user account.

**SecuritySize:**  The size, in bytes, of **SecurityDescriptor**.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that specifies the security settings for the user account object.

**DummyString2:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString3:**  See description for DummyString2.

**DummyString4:**  See description for DummyString2

**DummyLong1:**  The high part (the first 32 bits) of the **LastBadPasswordTime** field of the SAMPR\_USER\_INTERNAL3\_INFORMATION structure, as specified in [MS-SAMR] section 2.2.7.7.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_DELTA\_GROUP\_MEMBER

The NETLOGON\_DELTA\_GROUP\_MEMBER structure contains information about members of a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) by providing pointers to a list of group members and their respective attributes. This structure is used to replicate the group membership data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

All fields of this structure, except the fields detailed following the structure definition, have the same meanings as the identically named fields of the SAMPR\_GET\_MEMBERS\_BUFFER structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.3.14. The last four fields of the structure (DummyLong1, DummyLong2, DummyLong3, and DummyLong4) are not found in [MS-SAMR].

1. typedef struct \_NETLOGON\_DELTA\_GROUP\_MEMBER {
2. [size\_is(MemberCount)] ULONG \* Members;
3. [size\_is(MemberCount)] ULONG \* Attributes;
4. ULONG MemberCount;
5. ULONG DummyLong1;
6. ULONG DummyLong2;
7. ULONG DummyLong3;
8. ULONG DummyLong4;
9. } NETLOGON\_DELTA\_GROUP\_MEMBER,
10. \*PNETLOGON\_DELTA\_GROUP\_MEMBER;

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong3:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

**DummyLong4:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is specified in section 1.3.8.1.2.

##### NETLOGON\_DELTA\_ID\_UNION

The NETLOGON\_DELTA\_ID\_UNION union defines an account identifier type that is selected based on the requested [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) change.

1. typedef
2. [switch\_type(NETLOGON\_DELTA\_TYPE)]
3. union \_NETLOGON\_DELTA\_ID\_UNION {
4. [case(AddOrChangeDomain, AddOrChangeGroup, DeleteGroup, RenameGroup, AddOrChangeUser, DeleteUser, RenameUser, ChangeGroupMembership, AddOrChangeAlias, DeleteAlias, RenameAlias, ChangeAliasMembership, DeleteGroupByName, DeleteUserByName)]
5. ULONG Rid;
6. [case(AddOrChangeLsaPolicy, AddOrChangeLsaTDomain, DeleteLsaTDomain, AddOrChangeLsaAccount, DeleteLsaAccount)]
7. PRPC\_SID Sid;
8. [case(AddOrChangeLsaSecret, DeleteLsaSecret)]
9. [string] wchar\_t\* Name;
10. [default]  ;
11. } NETLOGON\_DELTA\_ID\_UNION,
12. \*PNETLOGON\_DELTA\_ID\_UNION;

**Rid:**  A 32-bit [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) whose type is selected when the following [**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e) types are switched: AddOrChangeDomain(1), AddOrChangeGroup(2), RenameGroup(4), DeleteGroup(3), AddOrChangeUser(5), DeleteUser(6), RenameUser(7), ChangeGroupMembership(8), AddOrChangeAlias(9), DeleteAlias(10), RenameAlias(11), ChangeAliasMembership(12), DeleteGroupByName(20), and DeleteUserByName(21).

**Sid:**  A pointer to a [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) whose type is selected when the following delta types are switched: AddOrChangeLsaPolicy(13), AddOrChangeLsaDomain(14), DeleteLsaTDomain(15), AddOrChangeLsaAccount(16), and DeleteLsaAccount(17).

**Name:**  A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains an identifier name. This identifier type is selected when the following delta types are switched: AddOrChangeLsaSecret(18) and DeleteLsaSecret(19).

##### NETLOGON\_DELTA\_POLICY

The NETLOGON\_DELTA\_POLICY structure contains information about the [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy. This structure is used for replicating the LSA policy data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

1. typedef struct \_NETLOGON\_DELTA\_POLICY {
2. ULONG MaximumLogSize;
3. OLD\_LARGE\_INTEGER AuditRetentionPeriod;
4. UCHAR AuditingMode;
5. ULONG MaximumAuditEventCount;
6. [size\_is(MaximumAuditEventCount + 1)]
7. ULONG \* EventAuditingOptions;
8. RPC\_UNICODE\_STRING PrimaryDomainName;
9. PRPC\_SID PrimaryDomainSid;
10. NLPR\_QUOTA\_LIMITS QuotaLimits;
11. OLD\_LARGE\_INTEGER ModifiedId;
12. OLD\_LARGE\_INTEGER DatabaseCreationTime;
13. SECURITY\_INFORMATION SecurityInformation;
14. ULONG SecuritySize;
15. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
16. RPC\_UNICODE\_STRING DummyString1;
17. RPC\_UNICODE\_STRING DummyString2;
18. RPC\_UNICODE\_STRING DummyString3;
19. RPC\_UNICODE\_STRING DummyString4;
20. ULONG DummyLong1;
21. ULONG DummyLong2;
22. ULONG DummyLong3;
23. ULONG DummyLong4;
24. } NETLOGON\_DELTA\_POLICY,
25. \*PNETLOGON\_DELTA\_POLICY;

**MaximumLogSize:**  This field has the same meaning as the identically named field of the POLICY\_AUDIT\_LOG\_INFO structure, as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.4.3.

**AuditRetentionPeriod:**  This field has the same meaning as the identically named field of the POLICY\_AUDIT\_LOG\_INFO structure, as specified in [MS-LSAD] section 2.2.4.3.

**AuditingMode:**  This field has the same meaning as the identically named field of the LSAPR\_POLICY\_AUDIT\_EVENTS\_INFO structure, as specified in [MS-LSAD] section 2.2.4.4.

**MaximumAuditEventCount:**  This field has the same meaning as the identically named field of the LSAPR\_POLICY\_AUDIT\_EVENTS\_INFO structure, as specified in [MS-LSAD] section 2.2.4.4.

**EventAuditingOptions:**  This field has the same meaning as the identically named field of the LSAPR\_POLICY\_AUDIT\_EVENTS\_INFO structure, as specified in [MS-LSAD] section 2.2.4.4.

**PrimaryDomainName:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496).

**PrimaryDomainSid:**  A pointer to the [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) for the primary domain.

**QuotaLimits:**  An NLPR\_QUOTA\_LIMITS structure, as specified in section [2.2.1.5.2](#Section_55d7ea86c4cc4a5e8414426673cb77d1), that contains information about system resource quotas imposed on an account.

**ModifiedId:**  An OLD\_LARGE\_INTEGER structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.2.2, that contains the count that is incremented each time the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) is modified. This count is the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) for the database.

**DatabaseCreationTime:**  A 64-bit time stamp, equivalent to a **FILETIME**, specifying when the database was created.

**SecurityInformation:**  A SECURITY\_INFORMATION bit flag that contains security information about the policy. For details about SECURITY\_INFORMATION structure, see [MS-DTYP] section 2.4.7.

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6, that describes the security settings for the LSA policy object.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NLPR\_CR\_CIPHER\_VALUE

The NLPR\_CR\_CIPHER\_VALUE structure defines an encrypted string buffer that contains the value of an [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) Secret Object as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc).

1. typedef struct \_NLPR\_CR\_CIPHER\_VALUE {
2. ULONG Length;
3. ULONG MaximumLength;
4. [size\_is(MaximumLength), length\_is(Length)]
5. UCHAR \* Buffer;
6. } NLPR\_CR\_CIPHER\_VALUE,
7. \*PNLPR\_CR\_CIPHER\_VALUE;

**Length:**  The length, in bytes, of the used portion of the buffer.

**MaximumLength:**  The maximum length, in bytes, of the buffer.

**Buffer:**  A pointer to a buffer that contains the secret data encrypted with the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) used on the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) between the client and the server exchanging this data structure. The encryption algorithm is [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) if the flag C is set in the negotiated flags between the client and the server as detailed in section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed); otherwise the encryption algorithm is DES.

##### NETLOGON\_DELTA\_SECRET

The NETLOGON\_DELTA\_SECRET structure contains information about the [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) secret object, as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc). This structure is used to replicate the LSA secret object data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC, as detailed in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

1. typedef struct \_NETLOGON\_DELTA\_SECRET {
2. NLPR\_CR\_CIPHER\_VALUE CurrentValue;
3. OLD\_LARGE\_INTEGER CurrentValueSetTime;
4. NLPR\_CR\_CIPHER\_VALUE OldValue;
5. OLD\_LARGE\_INTEGER OldValueSetTime;
6. SECURITY\_INFORMATION SecurityInformation;
7. ULONG SecuritySize;
8. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
9. RPC\_UNICODE\_STRING DummyString1;
10. RPC\_UNICODE\_STRING DummyString2;
11. RPC\_UNICODE\_STRING DummyString3;
12. RPC\_UNICODE\_STRING DummyString4;
13. ULONG DummyLong1;
14. ULONG DummyLong2;
15. ULONG DummyLong3;
16. ULONG DummyLong4;
17. } NETLOGON\_DELTA\_SECRET,
18. \*PNETLOGON\_DELTA\_SECRET;

**CurrentValue:**  An NLPR\_CR\_CIPHER\_VALUE structure, as specified in section [2.2.1.5.20](#Section_c6fcb4974b1045958fe796bf961ba292), that contains the encrypted current value of the LSA secret.

**CurrentValueSetTime:**  A 64-bit time stamp, equivalent to a **FILETIME**, at which the current value of the LSA secret object was set.

**OldValue:**  An NLPR\_CR\_CIPHER\_VALUE structure, as specified in section 2.2.1.5.20, that contains the encrypted previous (old) value of the LSA secret.

**OldValueSetTime:**  A 64-bit time stamp, equivalent to a **FILETIME**, at which the previous value of the LSA secret object was set.

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.7, that specifies portions of a security descriptor about the secret object.

**SecuritySize:**  The size, in bytes, of the **SecurityDescriptor** member.

**SecurityDescriptor:**  A pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6 that describes the security settings for the LSA secret object.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_DELTA\_TRUSTED\_DOMAINS

The NETLOGON\_DELTA\_TRUSTED\_DOMAINS structure contains information about a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). This structure is used for replicating the trusted domain data from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to a BDC.

1. typedef struct \_NETLOGON\_DELTA\_TRUSTED\_DOMAINS {
2. RPC\_UNICODE\_STRING DomainName;
3. ULONG NumControllerEntries;
4. [size\_is(NumControllerEntries)]
5. PRPC\_UNICODE\_STRING ControllerNames;
6. SECURITY\_INFORMATION SecurityInformation;
7. ULONG SecuritySize;
8. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
9. RPC\_UNICODE\_STRING DummyString1;
10. RPC\_UNICODE\_STRING DummyString2;
11. RPC\_UNICODE\_STRING DummyString3;
12. RPC\_UNICODE\_STRING DummyString4;
13. ULONG TrustedPosixOffset;
14. ULONG DummyLong2;
15. ULONG DummyLong3;
16. ULONG DummyLong4;
17. } NETLOGON\_DELTA\_TRUSTED\_DOMAINS,
18. \*PNETLOGON\_DELTA\_TRUSTED\_DOMAINS;

**DomainName:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the trusted domain.

**NumControllerEntries:**  Number of [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) names listed in the **ControllerNames** field.[<48>](#Appendix_A_48" \o "Product behavior note 48)

**ControllerNames:**  Pointer to an array of RPC\_UNICODE\_STRING structures, as specified in [MS-DTYP] section 2.3.10, that contain the NetBIOS names of the DCs in the trusted domain. The only restriction is the maximum value of the 32-bit unsigned integer enforced by [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331).[<49>](#Appendix_A_49" \o "Product behavior note 49)

**SecurityInformation:**  A SECURITY\_INFORMATION structure, as specified in [MS-DTYP] section 2.4.7, that specifies portions of a security descriptor about the trusted domain.

**SecuritySize:**  Size, in bytes, of the **SecurityDescriptor** field.

**SecurityDescriptor:**  Pointer to a SECURITY\_DESCRIPTOR structure, as specified in [MS-DTYP] section 2.4.6 that describes the security settings for the trusted domain object.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**TrustedPosixOffset:**  The value that contains the POSIX offset for the trusted domain, as specified in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.6.

**DummyLong2:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong3:**  See description for DummyLong2.

**DummyLong4:**  See description for DummyLong2.

##### NETLOGON\_RENAME\_ALIAS

The NETLOGON\_RENAME\_ALIAS structure specifies a rename of an [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd).

1. typedef struct \_NETLOGON\_DELTA\_RENAME\_ALIAS {
2. RPC\_UNICODE\_STRING OldName;
3. RPC\_UNICODE\_STRING NewName;
4. RPC\_UNICODE\_STRING DummyString1;
5. RPC\_UNICODE\_STRING DummyString2;
6. RPC\_UNICODE\_STRING DummyString3;
7. RPC\_UNICODE\_STRING DummyString4;
8. ULONG DummyLong1;
9. ULONG DummyLong2;
10. ULONG DummyLong3;
11. ULONG DummyLong4;
12. } NETLOGON\_RENAME\_ALIAS,
13. \*PNETLOGON\_DELTA\_RENAME\_ALIAS;

**OldName:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the previous name of the alias.

**NewName:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, that contains the new name to assign to the alias.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_RENAME\_GROUP

The NETLOGON\_RENAME\_GROUP structure specifies a rename of a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac).

1. typedef struct \_NETLOGON\_DELTA\_RENAME\_GROUP {
2. RPC\_UNICODE\_STRING OldName;
3. RPC\_UNICODE\_STRING NewName;
4. RPC\_UNICODE\_STRING DummyString1;
5. RPC\_UNICODE\_STRING DummyString2;
6. RPC\_UNICODE\_STRING DummyString3;
7. RPC\_UNICODE\_STRING DummyString4;
8. ULONG DummyLong1;
9. ULONG DummyLong2;
10. ULONG DummyLong3;
11. ULONG DummyLong4;
12. } NETLOGON\_RENAME\_GROUP,
13. \*PNETLOGON\_DELTA\_RENAME\_GROUP;

**OldName:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the group's previous name.

**NewName:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, that contains the new name to assign to the group.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:** See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NETLOGON\_RENAME\_USER

The NETLOGON\_RENAME\_USER structure specifies a rename of a user account.

1. typedef struct \_NETLOGON\_DELTA\_RENAME\_USER {
2. RPC\_UNICODE\_STRING OldName;
3. RPC\_UNICODE\_STRING NewName;
4. RPC\_UNICODE\_STRING DummyString1;
5. RPC\_UNICODE\_STRING DummyString2;
6. RPC\_UNICODE\_STRING DummyString3;
7. RPC\_UNICODE\_STRING DummyString4;
8. ULONG DummyLong1;
9. ULONG DummyLong2;
10. ULONG DummyLong3;
11. ULONG DummyLong4;
12. } NETLOGON\_RENAME\_USER,
13. \*PNETLOGON\_DELTA\_RENAME\_USER;

**OldName:**  An RPC\_UNICODE\_STRING structure, as specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.10, that contains the user account's previous name.

**NewName:**  An RPC\_UNICODE\_STRING structure, as specified in [MS-DTYP] section 2.3.10, that contains the new name to assign to the user account.

**DummyString1:**  A STRING structure, defined in section [2.2.1.1.2](#Section_4a896c09a39c487894f09e4f8a419f32), that MUST contain 0 for the **Length** field, 0 for the **MaximumLength** field, and NULL for the **Buffer** field. It is ignored upon receipt. The Netlogon usage of dummy fields is described in section [1.3.8.1.2](#Section_bbc95890215e49a98bb892e723548046).

**DummyString2:**  See description for DummyString1.

**DummyString3:**  See description for DummyString1.

**DummyString4:**  See description for DummyString1.

**DummyLong1:**  MUST be set to zero and MUST be ignored on receipt. The Netlogon usage of dummy fields is described in section 1.3.8.1.2.

**DummyLong2:**  See description for DummyLong1.

**DummyLong3:**  See description for DummyLong1.

**DummyLong4:**  See description for DummyLong1.

##### NLPR\_MODIFIED\_COUNT

The NLPR\_MODIFIED\_COUNT structure specifies a count for the number of times an account's [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) has been modified.

1. typedef struct \_NLPR\_MODIFIED\_COUNT {
2. OLD\_LARGE\_INTEGER ModifiedCount;
3. } NLPR\_MODIFIED\_COUNT,
4. \*PNLPR\_MODIFIED\_COUNT;

**ModifiedCount:**  An OLD\_LARGE\_INTEGER structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.2.2, that contains the number of modifications made to the database since its creation. This value is the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d).

##### NETLOGON\_DELTA\_UNION

The NETLOGON\_DELTA\_UNION union defines a union of all types of [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) changes ([**deltas**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e)).

1. typedef
2. [switch\_type(NETLOGON\_DELTA\_TYPE)]
3. union \_NETLOGON\_DELTA\_UNION {
4. [case(AddOrChangeDomain)]
5. PNETLOGON\_DELTA\_DOMAIN DeltaDomain;
6. [case(AddOrChangeGroup)]
7. PNETLOGON\_DELTA\_GROUP DeltaGroup;
8. [case(RenameGroup)]
9. PNETLOGON\_DELTA\_RENAME\_GROUP DeltaRenameGroup;
10. [case(AddOrChangeUser)]
11. PNETLOGON\_DELTA\_USER DeltaUser;
12. [case(RenameUser)]
13. PNETLOGON\_DELTA\_RENAME\_USER DeltaRenameUser;
14. [case(ChangeGroupMembership)]
15. PNETLOGON\_DELTA\_GROUP\_MEMBER DeltaGroupMember;
16. [case(AddOrChangeAlias)]
17. PNETLOGON\_DELTA\_ALIAS DeltaAlias;
18. [case(RenameAlias)]
19. PNETLOGON\_DELTA\_RENAME\_ALIAS DeltaRenameAlias;
20. [case(ChangeAliasMembership)]
21. PNETLOGON\_DELTA\_ALIAS\_MEMBER DeltaAliasMember;
22. [case(AddOrChangeLsaPolicy)]
23. PNETLOGON\_DELTA\_POLICY DeltaPolicy;
24. [case(AddOrChangeLsaTDomain)]
25. PNETLOGON\_DELTA\_TRUSTED\_DOMAINS DeltaTDomains;
26. [case(AddOrChangeLsaAccount)]
27. PNETLOGON\_DELTA\_ACCOUNTS DeltaAccounts;
28. [case(AddOrChangeLsaSecret)]
29. PNETLOGON\_DELTA\_SECRET DeltaSecret;
30. [case(DeleteGroupByName)]
31. PNETLOGON\_DELTA\_DELETE\_GROUP DeltaDeleteGroup;
32. [case(DeleteUserByName)]
33. PNETLOGON\_DELTA\_DELETE\_USER DeltaDeleteUser;
34. [case(SerialNumberSkip)]
35. PNLPR\_MODIFIED\_COUNT DeltaSerialNumberSkip;
36. [default]  ;
37. } NETLOGON\_DELTA\_UNION,
38. \*PNETLOGON\_DELTA\_UNION;

**DeltaDomain:**  A pointer to a NETLOGON\_DELTA\_DOMAIN structure, as specified in section [2.2.1.5.10](#Section_803be876d7554187a011eaf5bf2755ab), that describes a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). This structure is selected when the delta type is AddOrChangeDomain.

**DeltaGroup:**  A pointer to a NETLOGON\_DELTA\_GROUP structure, as specified in section [2.2.1.5.13](#Section_b7949b4e0fc740d488418d69230e2d79), that describes a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) account. This structure is selected when the delta type is AddOrChangeGroup.

**DeltaRenameGroup:**  A pointer to a NETLOGON\_RENAME\_GROUP structure, as specified in section [2.2.1.5.24](#Section_c48a22162c51412baeb6c6666004b53f), that describes a rename of a group account. This structure is selected when the delta type is RenameGroup.

**DeltaUser:**  A pointer to a NETLOGON\_DELTA\_USER structure, as specified in section [2.2.1.5.16](#Section_c82fcc5a59b647f79f69dec916ebed2c), that describes a domain user account. This structure is selected when the delta type is AddOrChangeUser.

**DeltaRenameUser:**  A pointer to a NETLOGON\_RENAME\_USER structure, as specified in section [2.2.1.5.25](#Section_96943cc2441245df8ac0f4b3d323a27e), that describes a rename of a user account. This structure is selected when the delta type is RenameUser.

**DeltaGroupMember:**  A pointer to a NETLOGON\_DELTA\_GROUP\_MEMBER structure, as specified in section [2.2.1.5.17](#Section_3d4c56361f2a4896a717d8598ffaffab), that describes a group membership. This structure is selected when the delta type is ChangeGroupMembership.

**DeltaAlias:**  A pointer to a NETLOGON\_DELTA\_ALIAS structure, as specified in section [2.2.1.5.4](#Section_38155d03b5dc445d9fcba6938be5972d), that describes an [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd). This structure is selected when the delta type is AddOrChangeAlias.

**DeltaRenameAlias:**  A pointer to a NETLOGON\_RENAME\_ALIAS structure, as specified in section [2.2.1.5.23](#Section_15426b427d0740e4bca7933823d1b40e), that describes a rename of an alias. This structure is selected when the delta type is RenameAlias.

**DeltaAliasMember:**  A pointer to a NETLOGON\_DELTA\_ALIAS\_MEMBER structure, as specified in section [2.2.1.5.7](#Section_aeca74675e13417ca4cb71d1f6476090), that describes an alias membership. This structure is selected when the delta type is ChangeAliasMembership.

**DeltaPolicy:**  A pointer to a NETLOGON\_DELTA\_POLICY structure, as specified in section [2.2.1.5.19](#Section_b9ee3608efd14d57b4da5a13b9ec1fa1), that describes an [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy. This structure is selected when the delta type is AddOrChangeLsaPolicy.

**DeltaTDomains:**  A pointer to a NETLOGON\_DELTA\_TRUSTED\_DOMAINS structure, as specified in section [2.2.1.5.22](#Section_fe95340edb884fdd85c6bc8ad1c4ff8c), that describes a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain. This structure is selected when the delta type is AddOrChangeLsaTDomain.

**DeltaAccounts:**  A pointer to a NETLOGON\_DELTA\_ACCOUNTS structure, as specified in section [2.2.1.5.3](#Section_7f60a1a799d849ba91c06e027237b009), that describes an LSA account. This structure is selected when the delta type is AddOrChangeLsaAccount.

**DeltaSecret:**  A pointer to a NETLOGON\_DELTA\_SECRET structure, as specified in section [2.2.1.5.21](#Section_ddf4e131ef89425fa70b88fdd73afb51), that describes a LSA secret object as detailed in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc). This structure is selected when the delta type is AddOrChangeLsaSecret.

**DeltaDeleteGroup:**  A pointer to a NETLOGON\_DELTA\_DELETE\_GROUP structure, as specified in section [2.2.1.5.8](#Section_3ef0689005194f6e889dec76cd865d7c), that describes a group account deletion. This structure is selected when the delta type is DeleteGroupByName.

**DeltaDeleteUser:**  A pointer to a NETLOGON\_DELTA\_DELETE\_USER structure, as specified in section [2.2.1.5.9](#Section_3fb60f5fe33d427bb540ac3b84342d5d), that describes a user account deletion. This structure is selected when the delta type is DeleteUserByName.

**DeltaSerialNumberSkip:**  A pointer to an NLPR\_MODIFIED\_COUNT structure, as specified in section [2.2.1.5.26](#Section_75dd36998abc45d29fb7e7a9a78779f5), that holds the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d). This structure is selected when the delta type is SerialNumberSkip.

##### NETLOGON\_DELTA\_TYPE

The NETLOGON\_DELTA\_TYPE enumeration defines an enumerated set of possible [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) changes.

1. typedef enum \_NETLOGON\_DELTA\_TYPE
2. {
3. AddOrChangeDomain = 1,
4. AddOrChangeGroup = 2,
5. DeleteGroup = 3,
6. RenameGroup = 4,
7. AddOrChangeUser = 5,
8. DeleteUser = 6,
9. RenameUser = 7,
10. ChangeGroupMembership = 8,
11. AddOrChangeAlias = 9,
12. DeleteAlias = 10,
13. RenameAlias = 11,
14. ChangeAliasMembership = 12,
15. AddOrChangeLsaPolicy = 13,
16. AddOrChangeLsaTDomain = 14,
17. DeleteLsaTDomain = 15,
18. AddOrChangeLsaAccount = 16,
19. DeleteLsaAccount = 17,
20. AddOrChangeLsaSecret = 18,
21. DeleteLsaSecret = 19,
22. DeleteGroupByName = 20,
23. DeleteUserByName = 21,
24. SerialNumberSkip = 22
25. } NETLOGON\_DELTA\_TYPE;

**AddOrChangeDomain:** Adds or changes a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**Security Account Manager (SAM)**](#gt_0b53d5bb-74ab-4705-8657-c22d32781103) account.

**AddOrChangeGroup:** Adds or changes a [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) SAM account.

**DeleteGroup:** Deletes a group SAM account.

**RenameGroup:** Renames a group SAM account.

**AddOrChangeUser:** Adds or changes a user SAM account.

**DeleteUser:** Deletes a user SAM account.

**RenameUser:** Renames a user SAM account.

**ChangeGroupMembership:** Changes a group membership record.

**AddOrChangeAlias:** Adds or changes an [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd).

**DeleteAlias:** Deletes an alias.

**RenameAlias:** Renames an alias.

**ChangeAliasMembership:** Changes the membership record for an alias.

**AddOrChangeLsaPolicy:** Adds or changes an [**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) policy.

**AddOrChangeLsaTDomain:** Adds or changes a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain account**](#gt_d0be6ce0-cc28-43cd-bd6b-6f324fcb8397).

**DeleteLsaTDomain:** Deletes a trusted domain account.

**AddOrChangeLsaAccount:** Adds or changes an LSA user or machine account.

**DeleteLsaAccount:** Deletes an LSA user or machine account.

**AddOrChangeLsaSecret:** Adds or changes an LSA encrypted data block.

**DeleteLsaSecret:** Deletes an LSA encrypted data block.

The following three types MAY[<50>](#Appendix_A_50" \o "Product behavior note 50) have an additional requirement.

**DeleteGroupByName:** Deletes a group account based on a string name.

**DeleteUserByName:** Deletes a user account based on a string name.

**SerialNumberSkip:** Updates the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d).

##### SYNC\_STATE

The SYNC\_STATE enumeration tracks the progress of synchronization of the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) between BDCs and [**PDCs**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). Synchronization is initiated by the client calling [NetrDatabaseSync2 (section 3.5.4.6.2)](#Section_31fc80bd4f4d4512a792e488bb78f6a0). All references to *SyncContext* in the following synchronization state descriptions refer to the *SyncContext* parameter in that method.

1. typedef enum \_SYNC\_STATE
2. {
3. NormalState = 0,
4. DomainState = 1,
5. GroupState = 2,
6. UasBuiltInGroupState = 3,
7. UserState = 4,
8. GroupMemberState = 5,
9. AliasState = 6,
10. AliasMemberState = 7,
11. SamDoneState = 8
12. } SYNC\_STATE,
13. \*PSYNC\_STATE;

**NormalState:** A state that MUST be used unless the current synchronization is the restart of a full synchronization.

**DomainState:** The *SyncContext* parameter is the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) with which to continue.

**GroupState:** The *SyncContext* parameter is the global [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) RID with which to continue.

**UasBuiltInGroupState:** Not used.

**UserState:** The *SyncContext* parameter is the user RID with which to continue.

**GroupMemberState:** The *SyncContext* parameter is the global group RID with which to continue.

**AliasState:** The *SyncContext* parameter MUST have a value of 0, indicating synchronization restarts at the first database [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd) and that AddOrChangeAlias (see NETLOGON\_DELTA\_TYPE enumeration, [2.2.1.5.28](#Section_f8a8cd32426d45f1be45e0dc5c1c1359)) was the last account change being performed prior to the restart.

**AliasMemberState:** The *SyncContext* parameter MUST have a value of 0, indicating synchronization restarts at the first database alias and that ChangeAliasMembership (see NETLOGON\_DELTA\_TYPE enumeration, 2.2.1.5.28) was the last account change being performed prior to the restart.

**SamDoneState:** The database has finished synchronization.

#### Domain Trust Structures

Structures in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used for retrieving [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) information as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### DOMAIN\_NAME\_BUFFER

The DOMAIN\_NAME\_BUFFER structure defines information returned by the [NetrEnumerateTrustedDomains](#Section_1d106b28c30f4fd1b7b0240b6250d7f6) method, as specified in section 3.5.4.7.3. The structure is used to describe a set of [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain names**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c).

1. typedef struct \_DOMAIN\_NAME\_BUFFER {
2. ULONG DomainNameByteCount;
3. [unique, size\_is(DomainNameByteCount)]
4. UCHAR \* DomainNames;
5. } DOMAIN\_NAME\_BUFFER,
6. \*PDOMAIN\_NAME\_BUFFER;

**DomainNameByteCount:**  The size, in bytes, of the buffer pointed to by the **DomainNames** field, including all UTF-16 null characters.

**DomainNames:**  The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string buffer that contains the list of trusted [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). The list format is a UTF-16 string composed of one or more substrings. Each substring is separated from adjacent substrings by the UTF-16 null character, 0x0000. After the final substring, the string is terminated by two UTF-16 null characters.

For example, if there are three trusted domains, DOMAIN1, DOMAIN2, and DOMAIN3, the **DomainNames** string buffer would have the following form:

DOMAIN1<null>DOMAIN2<null>DOMAIN3<null><null>

where <null> is the UTF-16 null character, 0x0000.

##### DS\_DOMAIN\_TRUSTSW

The DS\_DOMAIN\_TRUSTSW structure defines information about a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6). It is part of the [NETLOGON\_TRUSTED\_DOMAIN\_ARRAY](#Section_251cf1be29324d338532595cf42e8091) structure returned by the [DsrEnumerateDomainTrusts](#Section_f98236242b34415cbdca9f9a6d97016b) method, as specified in section 3.5.4.7.1. This structure SHOULD[<51>](#Appendix_A_51" \o "Product behavior note 51) contain naming information and trust-related information for a specific trusted domain.

1. typedef struct \_DS\_DOMAIN\_TRUSTSW {
2. [string] wchar\_t\* NetbiosDomainName;
3. [string] wchar\_t\* DnsDomainName;
4. ULONG Flags;
5. ULONG ParentIndex;
6. ULONG TrustType;
7. ULONG TrustAttributes;
8. PRPC\_SID DomainSid;
9. GUID DomainGuid;
10. } DS\_DOMAIN\_TRUSTSW,
11. \*PDS\_DOMAIN\_TRUSTSW;

**NetbiosDomainName:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the trusted domain.

**DnsDomainName:**  A pointer to a null-terminated Unicode string that contains the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e)of the trusted domain.

**Flags:**  A set of bit flags that defines the domain trust attributes. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | F | E | D | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Domain is a member of a [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). |
| B | Domain is directly trusted by the current domain. |
| C | Domain is the root of a forests. |
| D | Domain is the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) of the queried server. |
| E | Primary domain is running in native mode. |
| F | Domain directly trusts the current domain. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**ParentIndex:**  An integer value that contains the index in the NETLOGON\_TRUSTED\_DOMAIN\_ARRAY array (returned by the DsrEnumerateDomainTrusts method) that corresponds to the parent domain of the domain represented by this structure. This field is set if all of the following conditions are met:

* The A flag was specified in the *Flags* parameter of the DsrEnumerateDomainTrusts method.
* The **Flags** field of this structure, DS\_DOMAIN\_TRUSTSW, does not contain the C flag.

Otherwise, it MUST be set to zero and MUST be ignored.

**TrustType:**  An integer value that describes the type of domain with which the trust is associated. **TrustType** is one of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000001 | Trust is with a Windows NT domain.[<52>](#Appendix_A_52" \o "Product behavior note 52) |
| 0x00000002 | Trust is with an [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) domain.[<53>](#Appendix_A_53" \o "Product behavior note 53) |
| 0x00000003 | Trust is with an MIT Kerberos realm. |
| 0x00000004 | Trust is with a Distributed Computing Environment (DCE) realm. |

All other values MUST be ignored on receipt.

**TrustAttributes:**  A set of bit flags describing trust link attributes. A flag is true (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table, with the exception that bit F cannot be combined with E or D.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | I | H | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | G | F | E | D | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Trust link MUST NOT allow transitivity. |
| B | Trust link MAY[<54>](#Appendix_A_54" \o "Product behavior note 54) be valid. |
| C | Trust link MUST be set for [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) filtering of the client domain. For details about SID filtering, see [[MS-PAC]](%5bMS-PAC%5d.pdf#Section_166d8064c86341e19c23edaaa5f36962). |
| D | Trust link can contain [**forest trust information**](#gt_8c0b82d9-efec-4723-95a9-8564edf9ba44). |
| E | Trust link is to either a domain or a forest that is not part of the [**enterprise network**](#gt_e44ff7b5-53ad-4b0c-b82d-f4826008866f). |
| F | Trust link is internal to the forest. |
| G | Trust is to be treated as external for trust boundary purposes. |
| H | Domain is parent domain. |
| I | Domain is root of another forest. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**DomainSid:**  A pointer to an SID structure that identifies the current domain. If the **TrustType** field is set to C or D, the value is 0.

**DomainGuid:**  A [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) that identifies the current domain.

##### NETLOGON\_TRUSTED\_DOMAIN\_ARRAY

The NETLOGON\_TRUSTED\_DOMAIN\_ARRAY structure SHOULD[<55>](#Appendix_A_55" \o "Product behavior note 55) define information returned by the [NetrEnumerateTrustedDomainsEx](#Section_c3e9870a09434d45be94edb9419a1c11) method, as specified in section 3.5.4.7.2. It contains an array of [DS\_DOMAIN\_TRUSTSW](#Section_7de9866ed3ef4a9f98a5c2dcff1e61c1) structures, as specified in section 2.2.1.6.2, that describe [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) by the server processing the call.

1. typedef struct \_NETLOGON\_TRUSTED\_DOMAIN\_ARRAY {
2. DWORD DomainCount;
3. [size\_is(DomainCount)] PDS\_DOMAIN\_TRUSTSW Domains;
4. } NETLOGON\_TRUSTED\_DOMAIN\_ARRAY,
5. \*PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY;

**DomainCount:**  The number of entries in the **Domains** field.

**Domains:**   The data structure that contains an array of DS\_DOMAIN\_TRUSTSW structures, as specified in section 2.2.1.6.2, that represent trusted domains.

##### NL\_GENERIC\_RPC\_DATA

The NL\_GENERIC\_RPC\_DATA structure SHOULD[<56>](#Appendix_A_56" \o "Product behavior note 56) define a format for marshaling arrays of unsigned long values and [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) strings, by value, over [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331). The NL\_GENERIC\_RPC\_DATA structure can be used to transmit generic data over RPC from the server to a client.

1. typedef struct \_NL\_GENERIC\_RPC\_DATA {
2. ULONG UlongEntryCount;
3. [size\_is(UlongEntryCount)] ULONG \* UlongData;
4. ULONG UnicodeStringEntryCount;
5. [size\_is(UnicodeStringEntryCount)]
6. PRPC\_UNICODE\_STRING UnicodeStringData;
7. } NL\_GENERIC\_RPC\_DATA,
8. \*PNL\_GENERIC\_RPC\_DATA;

**UlongEntryCount:**   The number of entries in **UlongData**.

**UlongData:**   A pointer to an array of unsigned 32-bit integer values.

**UnicodeStringEntryCount:**   The number of entries in **UnicodeStringData**.

**UnicodeStringData:**  A pointer to an array of Unicode string structures.

#### Administrative Services Structures

Structures in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used to query and control Netlogon behavior, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NETLOGON\_CONTROL\_DATA\_INFORMATION

The NETLOGON\_CONTROL\_DATA\_INFORMATION union is used as input to the [NetrLogonControl2](#Section_650a105f64434eb0839a188708328fb0) method, as specified in section 3.5.4.9.2, and the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method, as specified in section 3.5.4.9.1. This union selects a data type, based on the FunctionCode parameter passed to the method. For details about FunctionCode values, see NetrLogonControl2Ex, section 3.5.4.9.1.

1. typedef
2. [switch\_type(DWORD)]
3. union \_NETLOGON\_CONTROL\_DATA\_INFORMATION {
4. [case(5,6,9,10)]
5. [string] wchar\_t\* TrustedDomainName;
6. [case(65534)]
7. DWORD DebugFlag;
8. [case(8)]
9. [string] wchar\_t\* UserName;
10. [default]  ;
11. } NETLOGON\_CONTROL\_DATA\_INFORMATION,
12. \*PNETLOGON\_CONTROL\_DATA\_INFORMATION;

**TrustedDomainName:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c). Switched on the DWORD ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.2.9) values 0x00000005, 0x00000006, 0x00000009, and 0x0000000A. The DWORD values are equivalent to FunctionCode values. For a complete list of the Netlogon function codes and their associated meanings, see NetrLogonControl2Ex, section 3.5.4.9.1.

**DebugFlag:**  A DWORD that contains an implementation-specific debug flag. Switched on the value 0x0000FFFE.

**UserName:**  A pointer to null-terminated Unicode string that contains a user name. Switched on the DWORD value 0x00000008.

##### NETLOGON\_INFO\_1

The NETLOGON\_INFO\_1 structure defines information returned as part of an administrative query, as detailed in the description of the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method in section 3.5.4.9.1. This structure is used to convey information about the state and properties of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) of the queried server. Additionally, this structure MAY[<57>](#Appendix_A_57" \o "Product behavior note 57) contain information about the state of the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) synchronization.

1. typedef struct \_NETLOGON\_INFO\_1 {
2. DWORD netlog1\_flags;
3. NET\_API\_STATUS netlog1\_pdc\_connection\_status;
4. } NETLOGON\_INFO\_1,
5. \*PNETLOGON\_INFO\_1;

**netlog1\_flags:**  A set of bit flags that are defined in the following table. A flag SHOULD[<58>](#Appendix_A_58" \o "Product behavior note 58) be TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | G | F | E | D | C | B | A |

| Value | Description |
| --- | --- |
| A | One of the databases is out-of-date, and replication is needed. |
| B | At least one of the databases is currently being replicated. |
| C | At least one of the databases requires a full synchronization update. |
| D | At least one database record requires an update. |
| E | The DC used on the secure channel is reachable over TCP/IP. If this flag is not set, then the DC does not have a known IP address. |
| F | The DC used on the secure channel runs [**W32Time**](#gt_43e51d0a-ac6a-4662-a99a-8f3029b78caf). |
| G | The last update of one of the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) records on the DC failed. |

All other bits MUST be set to zero and MUST be ignored on receipt.

To a client, bit D will appear arbitrarily set to 0 or 1 and the client is not expected to perform any action based on this value. For more information, see the server to server database synchronization topic in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

**netlog1\_pdc\_connection\_status:**  The integer value that indicates the connection status (section [3.4.5.3.1](#Section_739115d00d16460f96c8775fde606bd5)) of the secure channel to a DC in the primary domain of the queried server. See section 3.4.5.3.1 for more information.

##### NETLOGON\_INFO\_2

The NETLOGON\_INFO\_2 structure defines information returned as part of an administrative query of the status of the Netlogon server, as detailed in the description of the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method in section 3.5.4.9.1. This structure is used to convey information about the status and properties of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the primary or directly [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) specified by the caller of the NetrLogonControl2Ex method.

1. typedef struct \_NETLOGON\_INFO\_2 {
2. DWORD netlog2\_flags;
3. NET\_API\_STATUS netlog2\_pdc\_connection\_status;
4. [string] wchar\_t\* netlog2\_trusted\_dc\_name;
5. NET\_API\_STATUS netlog2\_tc\_connection\_status;
6. } NETLOGON\_INFO\_2,
7. \*PNETLOGON\_INFO\_2;

**netlog2\_flags:**  A set of bit flags describing the following control query responses from the DC. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | 0 | B | A | 0 | 0 | 0 | 0 |

Where the flags SHOULD[<59>](#Appendix_A_59" \o "Product behavior note 59) be defined as shown in the following table.

| Value | Description |
| --- | --- |
| A | The DC used on the secure channel has an IP address (either IPv4 or IPv6). |
| B | The DC used on the secure channel runs [**W32Time**](#gt_43e51d0a-ac6a-4662-a99a-8f3029b78caf). |
| C | Signifies that the trust verification status was returned in the netlog2\_pdc\_connection\_status field. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**netlog2\_pdc\_connection\_status:**  Unless the C bit is set in **netlog2\_flags** field, this field indicates the connection status (section [3.4.5.3.1](#Section_739115d00d16460f96c8775fde606bd5)) of the secure channel to a DC in the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) of the queried server. If the C bit is set in **netlog2\_flags** field, this field indicates the connection status of verifying the secure channel to the DC in the specified domain (specified by the caller of the NetrLogonControl2Ex method; see section 3.5.4.9.1 for more information).

**netlog2\_trusted\_dc\_name:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the DC used on the secure channel for the specified domain. The name is the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) if the DC was discovered using the discovery mechanism based on the DNS query and LDAP ping ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.3). The name is the NetBIOS name if the DC was discovered using the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78)-based mechanism ([MS-ADTS] section 6.3.5).

**netlog2\_tc\_connection\_status:**  An integer value that indicates the connection status (section 3.4.5.3.1) of the secure channel to the DC in the specified domain.

##### NETLOGON\_INFO\_3

The NETLOGON\_INFO\_3 structure defines information returned as part of an administrative query of the status of the Netlogon server, as detailed in the description of the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method in section 3.5.4.9.1. This structure is used to return the number of NTLM logons attempted on the queried server since the last restart.

1. typedef struct \_NETLOGON\_INFO\_3 {
2. DWORD netlog3\_flags;
3. DWORD netlog3\_logon\_attempts;
4. DWORD netlog3\_reserved1;
5. DWORD netlog3\_reserved2;
6. DWORD netlog3\_reserved3;
7. DWORD netlog3\_reserved4;
8. DWORD netlog3\_reserved5;
9. } NETLOGON\_INFO\_3,
10. \*PNETLOGON\_INFO\_3;

**netlog3\_flags:**  MUST be set to zero and MUST be ignored on receipt.

**netlog3\_logon\_attempts:**  The number of NTLM logon attempts made on the server since the last restart.

**netlog3\_reserved1:**  MUST be set to zero and MUST be ignored on receipt.

**netlog3\_reserved2:**   MUST be set to zero and MUST be ignored on receipt.

**netlog3\_reserved3:**  MUST be set to zero and MUST be ignored on receipt.

**netlog3\_reserved4:**  MUST be set to zero and MUST be ignored on receipt.

**netlog3\_reserved5:**  MUST be set to zero and MUST be ignored on receipt.

##### NETLOGON\_INFO\_4

The NETLOGON\_INFO\_4 structure defines information that is returned as part of an administrative query of the status of the Netlogon server, as detailed in the description of the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method in section 3.5.4.9.1. This structure is used to convey information about the status and properties of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the primary or directly [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) containing the user account specified by the caller of the NetrLogonControl2Ex method.

1. typedef struct \_NETLOGON\_INFO\_4 {
2. [string] wchar\_t\* netlog4\_trusted\_dc\_name;
3. [string] wchar\_t\* netlog4\_trusted\_domain\_name;
4. } NETLOGON\_INFO\_4,
5. \*PNETLOGON\_INFO\_4;

**netlog4\_trusted\_dc\_name:**  A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of a DC that is used on the secure channel for the primary or directly trusted domain containing the specified user account. The name is the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) if the DC was discovered using the discovery mechanism based on the DNS query and LDAP ping ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.3). The name is the NetBIOS name if the DC was discovered using the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78)-based mechanism ([MS-ADTS] section 6.3.5).

**netlog4\_trusted\_domain\_name:**  A pointer to a null-terminated Unicode string that contains the NetBIOS name of the primary or directly trusted domain containing the specified user account.

##### NETLOGON\_CONTROL\_QUERY\_INFORMATION

The NETLOGON\_CONTROL\_QUERY\_INFORMATION union selects an appropriate **NETLOGON\_INFO** data type, based on the value of the *QueryLevel* parameter to the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method described in section 3.5.4.9.1.

1. typedef
2. [switch\_type(DWORD)]
3. union \_NETLOGON\_CONTROL\_QUERY\_INFORMATION {
4. [case(1)]
5. PNETLOGON\_INFO\_1 NetlogonInfo1;
6. [case(2)]
7. PNETLOGON\_INFO\_2 NetlogonInfo2;
8. [case(3)]
9. PNETLOGON\_INFO\_3 NetlogonInfo3;
10. [case(4)]
11. PNETLOGON\_INFO\_4 NetlogonInfo4;
12. [default]  ;
13. } NETLOGON\_CONTROL\_QUERY\_INFORMATION,
14. \*PNETLOGON\_CONTROL\_QUERY\_INFORMATION;

**NetlogonInfo1:**  This field is selected when the switched DWORD ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.2.9) value is 1. For more details about [NETLOGON\_INFO\_1](#Section_afeb873c48264beba35cae73a708b108), see section 2.2.1.7.2.

**NetlogonInfo2:**  This field is selected when the switched DWORD value is 2. For more details about [NETLOGON\_INFO\_2](#Section_c48a87004c174afb8866f0cfc0c0a671), see section 2.2.1.7.3.

**NetlogonInfo3:**  This field is selected when the switched DWORD value is 3. For more details about [NETLOGON\_INFO\_3](#Section_be92a2cd950c4b268cd3475065406b92), see section 2.2.1.7.4.

**NetlogonInfo4:**  This field is selected when the switched DWORD value is 4. For more details about [NETLOGON\_INFO\_4](#Section_a2b4c31118314de6bf5efe8427323144), see section 2.2.1.7.5.

#### Obsolete Structures

The structures in this section SHOULD[<60>](#Appendix_A_60" \o "Product behavior note 60) be unsupported, but they are types associated with parameters in methods defined in section [3.4.5.8](#Section_c96e78b25b964002bf2f3d6297736edc) that are also obsolete.

##### NETLOGON\_VALIDATION\_UAS\_INFO

The NETLOGON\_VALIDATION\_UAS\_INFO structure was for the support of LAN Manager products and is beyond the scope of this document.

1. typedef struct \_NETLOGON\_VALIDATION\_UAS\_INFO {
2. [string] wchar\_t\* usrlog1\_eff\_name;
3. DWORD usrlog1\_priv;
4. DWORD usrlog1\_auth\_flags;
5. DWORD usrlog1\_num\_logons;
6. DWORD usrlog1\_bad\_pw\_count;
7. DWORD usrlog1\_last\_logon;
8. DWORD usrlog1\_last\_logoff;
9. DWORD usrlog1\_logoff\_time;
10. DWORD usrlog1\_kickoff\_time;
11. DWORD usrlog1\_password\_age;
12. DWORD usrlog1\_pw\_can\_change;
13. DWORD usrlog1\_pw\_must\_change;
14. [string] wchar\_t\* usrlog1\_computer;
15. [string] wchar\_t\* usrlog1\_domain;
16. [string] wchar\_t\* usrlog1\_script\_path;
17. DWORD usrlog1\_reserved1;
18. } NETLOGON\_VALIDATION\_UAS\_INFO,
19. \*PNETLOGON\_VALIDATION\_UAS\_INFO;

##### NETLOGON\_LOGOFF\_UAS\_INFO

The NETLOGON\_LOGOFF\_UAS\_INFO structure was for the support of LAN Manager products and is beyond the scope of this document.

1. typedef struct \_NETLOGON\_LOGOFF\_UAS\_INFO {
2. DWORD Duration;
3. USHORT LogonCount;
4. } NETLOGON\_LOGOFF\_UAS\_INFORMATION,
5. \*PNETLOGON\_LOGOFF\_UAS\_INFO;

##### UAS\_INFO\_0

The UAS\_INFO\_0 structure was for the support of LAN Manager products and is beyond the scope of this document.

1. typedef struct \_UAS\_INFO\_0 {
2. CHAR ComputerName[16];
3. ULONG TimeCreated;
4. ULONG SerialNumber;
5. } UAS\_INFO\_0,
6. \*PUAS\_INFO\_0;

##### NETLOGON\_DUMMY1

The NETLOGON\_DUMMY1 union MAY[<61>](#Appendix_A_61" \o "Product behavior note 61) serve as a placeholder.

1. typedef
2. [switch\_type(DWORD)]
3. union {
4. [case(1)]
5. ULONG Dummy;
6. } NETLOGON\_DUMMY1,
7. \*PNETLOGON\_DUMMY1;

**Dummy:**  The field is selected when the switched DWORD ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.2.9) value is 1.

## Directory Service Schema Elements Used by the Netlogon Remote Protocol

The Netlogon Remote Protocol accesses the [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e) schema classes and attributes listed in the following table.

For the syntactic specifications of the following <Class> or <Class><Attribute> pairs, refer to Active Directory Domain Services (AD DS) ([[MS-ADA1]](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f), [[MS-ADA3]](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0), and [[MS-ADSC]](%5bMS-ADSC%5d.pdf#Section_9abb5e97123d4da99557b353ab79b830)).

| Class | Attribute |
| --- | --- |
| nTDSDSA | objectGUID |
| trustedDomain | trustAuthIncoming  trustAuthOutgoing |
| computer | lmPwdHistory  operatingSystem  securityIdentifier  operatingSystemVersion  servicePrincipalName  unicodePwd  dnsHostName |

# Protocol Details

The Netlogon Remote Protocol [**remote procedure call (RPC)**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) interface is used primarily to maintain the relationship between a machine and its [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), and relationships among [**domain controllers (DCs)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) and domains. As such, there are several distinct responsibilities that the RPC interface fulfills while acting in this maintenance capacity. These responsibilities are as follows:[<62>](#Appendix_A_62" \o "Product behavior note 62)

* To establish and maintain the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) that is used by members of a domain to communicate with the domain controller (DC).
* To transport authentication requests from [**domain members**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) to the DC, and among DCs. This functionality is most commonly implemented by authentications using the NTLM Authentication Protocol ([[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4)), but it is also used by other protocols such as Kerberos and Digest ([[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 1.4).
* To transmit certain account changes, such as password changes or account lockout information. Details about the types of account changes that can be transmitted are as specified in [Netlogon NT Replication Details (section 3.6)](#Section_f28f9dc8eeb241129eeca466f639c761).
* To serve as its own [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) for its RPC connection; that is, the authentication protocol is used both within the RPC exchanges for specific methods, and also as a general authentication protocol for the entire Netlogon Remote Protocol RPC interface.

The details of the Netlogon Remote Protocol are presented in the following sections:

* Section [3.1](#Section_273b6905782d4a7ea2e44337816916e0) specifies the authentication aspects that are common to all Netlogon Remote Protocol roles, including establishing the secure channel. Before any method that utilizes the secure channel can be invoked, the authentication process that is described in this section MUST be completed.
* Section [3.2](#Section_8ea3ca7111074888b108f5bdcb350eea) specifies the use of the Netlogon Remote Protocol for pass-through authentication.
* Section [3.3](#Section_388e4b68f4e44e0498ecdfae7e9b1f01) specifies the use of the Netlogon Remote Protocol authentication method as a generic security authentication mechanism.
* Sections [3.4](#Section_2e745bde2f654857bd3c7de7b191c35a) and [3.5](#Section_1b79123d2f1e4970b9e8ea74ba95f95a) detail client and server operations, respectively.
* Section 3.6 specifies the behavior of the Netlogon Remote Protocol in the account replication role in environments with BDCs.

All the Netlogon Remote Protocol methods return 0x00000000 (NERR\_Success) to indicate success; otherwise, they return a 32-bit nonzero error code. There are two types of error codes returned, NET\_API\_STATUS ([[MS-ERREF]](%5bMS-ERREF%5d.pdf#Section_1bc92ddfb79e413cbbaa99a5281a6c90) section 2.2) and NTSTATUS ([MS-ERREF] section 2.3). For more information about NTSTATUS values, see [[NTSTATUSERR]](https://go.microsoft.com/fwlink/?LinkId=90238).

**Common Error Processing Rules**

Several Netlogon Remote Protocol methods apply the processing rules listed in the following section to determine which error codes are returned. The applicable processing rules from those mentioned in this section are referred to in each of the method descriptions. Error codes prepended with the prefix STATUS are of type NTSTATUS; the remaining error codes are of type NET\_API\_STATUS.

| Common Error Processing Rule | Description |
| --- | --- |
| **A** | If a server does not support a specific Netlogon RPC method, it MUST return ERROR\_NOT\_SUPPORTED or STATUS\_NOT SUPPORTED, based on the return type. This includes the case when the server is not a domain controller. |
| **B** | If the input parameter to a Netlogon RPC request is a [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b) or server name, the server SHOULD[<63>](#Appendix_A_63" \o "Product behavior note 63) look up this name in the domain the server hosts. If the name is not found, the server MUST return ERROR\_INVALID\_COMPUTERNAME or STATUS\_INVALID\_COMPUTER\_NAME. |
| **C** | If a server needs to locate a domain controller (DC) to service a Netlogon RPC request, it follows the method specified in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6. If the DC cannot be located by following this method, the server MUST return ERROR\_NO\_LOGON\_SERVERS or STATUS\_NO\_LOGON\_SERVERS, depending on the return type. |
| **D** | If the [**Directory Service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e) is paused and the Netlogon RPC method cannot be processed further, the server SHOULD return STATUS\_DS\_BUSY. |
| **E** | The server MUST return ERROR\_NO\_SUCH\_DOMAIN if the DC could not be located for the specified domain, or if the specified domain is not primary or directly [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6). |

The default pointer type for the Netlogon Remote Protocol RPC interface is pointer\_default(unique). Method calls are received at a dynamically assigned [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee) ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.3.3.1.4). The endpoints for the Netlogon Remote Protocol service are negotiated by the RPC endpoint mapper ([MS-RPCE] section 3.3.3.3.1.4).

**Out of Memory Errors**

Netlogon Remote Protocol methods require allocation of memory in order to execute their processing rules. If a client or server is unable to allocate the memory required, it MUST return STATUS\_NO\_MEMORY.

## Netlogon Common Authentication Details

The Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) interface is used to establish and maintain the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca). The client MUST attempt to establish this secure channel with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) within the client's [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). (Common Error Processing Rule C MUST be applied whenever a secure connection to a DC is required by a method.) Establishing the secure channel is accomplished by first negotiating a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) (as specified in section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9)) over nonprotected RPC (nonprotected RPC is an RPC connection without any underlying security support), resulting in both the client and server mutually verifying each other's [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8). Verifying Netlogon credentials on both the client and server establishes that both ends shared the same password information for the requesting client. Therefore, both Netlogon credentials are valid. The client and server both store a copy of the Netlogon credential computed by using the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473). This stored client Netlogon credential serves as a seed for authenticating further client-to-server operations.

Upon successful mutual verification, both client and server have the information necessary to compute a session key. The session key is used to secure further RPC communication between the two machines.

The following sections specify the common steps in the authentication portion of the Netlogon RPC interface, including Netlogon credential computation and the derivation and use of the session key.

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

The Netlogon interface is used to create a secure connection between a client and a server, where the server is a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). The client of the Netlogon interface can be a member of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca), another DC in the same domain, or a DC in a different but [**trusting**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain. This secure connection is often referred to as the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca).

The connection is secured by the use of cryptographic algorithms. The key used for these algorithms, the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d), is computed on both the client and the server and is based on a [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) that has been previously shared between the client and the server. After the session key is computed on both sides, it is used to encrypt the communication between the two parties. There are two methods of deriving the key. The method used is version-dependent, as specified in section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63).

Abstract variables of the session key operations are as follows:

**ClientStoredCredential:** A [NETLOGON\_CREDENTIAL (section 2.2.1.3.4)](#Section_d55e263271634f6cb6624b870e8cc1cd) structure containing the [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) that is created by the client and received by the server and that is used during computation and verification of the Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)).

**ClientChallenge:** A pointer to a NETLOGON\_CREDENTIAL structure that contains the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473).

**NegotiateFlags:** A 32-bit set of bit flags that identify the negotiated capabilities between the client and the server.

**ServerStoredCredential:** A NETLOGON\_CREDENTIAL structure containing the credential that is created by the server and received by the client and that is used during computation and verification of the Netlogon authenticator.

**ServerChallenge:** A pointer to a NETLOGON\_CREDENTIAL structure that contains the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9) response.

**SharedSecret:** An even-numbered sequence of bytes, with no embedded zero values, that is a plain-text secret (password) shared between the client and the server. Implementers can choose to store the **unicodePwd** ([[MS-ADA3]](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0) section 2.332) instead of a clear text version of the shared secret.[<64>](#Appendix_A_64" \o "Product behavior note 64)[<65>](#Appendix_A_65" \o "Product behavior note 65)[<66>](#Appendix_A_66" \o "Product behavior note 66) For more information, refer to the ADM element **Password** in [[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) section 3.2.1.6; initialization of this shared ADM element is covered in the domain join and unjoin sections of [MS-WKST] (sections 3.2.4.13 and 3.2.4.14).

**TrustPasswordVersion:** An unsigned 32-bit integer that indicates the number of times that a trust password has changed.[<67>](#Appendix_A_67" \o "Product behavior note 67)

**SealSecureChannel:** A Boolean setting that indicates whether the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) message has to be encrypted or just integrity-protected ([[C706]](https://go.microsoft.com/fwlink/?LinkId=89824) section 13.2.5). When TRUE, the message will be encrypted; otherwise, it will be integrity-protected.

**StrongKeySupport:** A Boolean setting that indicates whether a strong method of creating the session key will be used. A strong method, in the context of Netlogon, is one that uses the MD5 message-digest algorithm [[RFC1321]](https://go.microsoft.com/fwlink/?LinkId=90275). The behavior of this setting is specified in section 3.1.4.3.

The Netlogon client and server variables are as follows:

**LocatedDCsCache:** A cache SHOULD be implemented containing a set of previously located DCs. The fields of the cache are implementation-specific but are required to contain enough information to be able to respond correctly to a DC locator request. Any cache implementation MUST be able to return the set of cache results given a [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c). The results SHOULD be equivalent to the DOMAIN\_CONTROLLER\_INFOW structure. Also, each entry SHOULD maintain, and return with any cache lookup, two timestamps. The first timestamp indicates when the entry was created so that age checks can be performed in order to invalidate stale cache entries. The second timestamp indicates the last communication with the indicated machine in order to facilitate periodic liveliness tests with the cached DC (see section [3.5.4.3.1](#Section_fb8e1146a0454c3198d1c68507ad5620) for more information).

**SealSecureChannel:** A Boolean setting that indicates whether the RPC message has to be encrypted or just integrity-protected ([C706] section 13.2.5). When TRUE, the message will be encrypted; otherwise, it will be integrity-protected.

Implementations SHOULD[<68>](#Appendix_A_68" \o "Product behavior note 68) persistently store and retrieve the **SealSecureChannel** variable.

The implementation SHOULD also expose the key and value at the specified registry path using the Windows Remote Registry Protocol [[MS-RRP]](%5bMS-RRP%5d.pdf#Section_0fa3191dbb79490a81bd54c2601b7a78). For each abstract data model (ADM) element that is loaded from the registry, there is one instance that is shared between the Windows Remote Registry Protocol and the protocol(s) that use the ADM element. Any changes made to the registry keys will be reflected in the ADM elements when a PolicyChange event is received ([[MS-GPOD]](%5bMS-GPOD%5d.pdf#Section_6e6349392ccf4412b75f0035dc05ea67) section 2.8.2).

### Timers

None.

### Initialization

See section [3.4.3](#Section_8db09e2864ff45a78219943405a74b56) for client initialization, and see section [3.5.3](#Section_f8c12682fd984c1a8b0ab6e153f96186) for server initialization.

### Message Processing Events and Sequencing Rules

Netlogon communication between a client and a server occurs through [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) calls. A subset of the methods defined by Netlogon's RPC interface requires a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to be established between the client and the server before these methods are called. Section [3.1.4.6](#Section_f61c3f4a53ff4f3090066d93a2162ef8) lists all Netlogon methods that require a session key. This section also specifies the sequence of steps that a client MUST follow when calling any method in the list. Section [3.1.4.7](#Section_6b7f7a1c83b7452c9b7b2ece221e236d) specifies the required sequence of steps that a client MUST follow when calling methods that do not require a session key. Section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63) specifies how the session key is computed. Section [3.1.4.10](#Section_00ac739d274d434b9efbfad10405721a) specifies how a client attempts to locate a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

#### Session-Key Negotiation

[**Session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation between a client and a server is performed over an unprotected [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) channel.

The following diagram illustrates the negotiation flow.

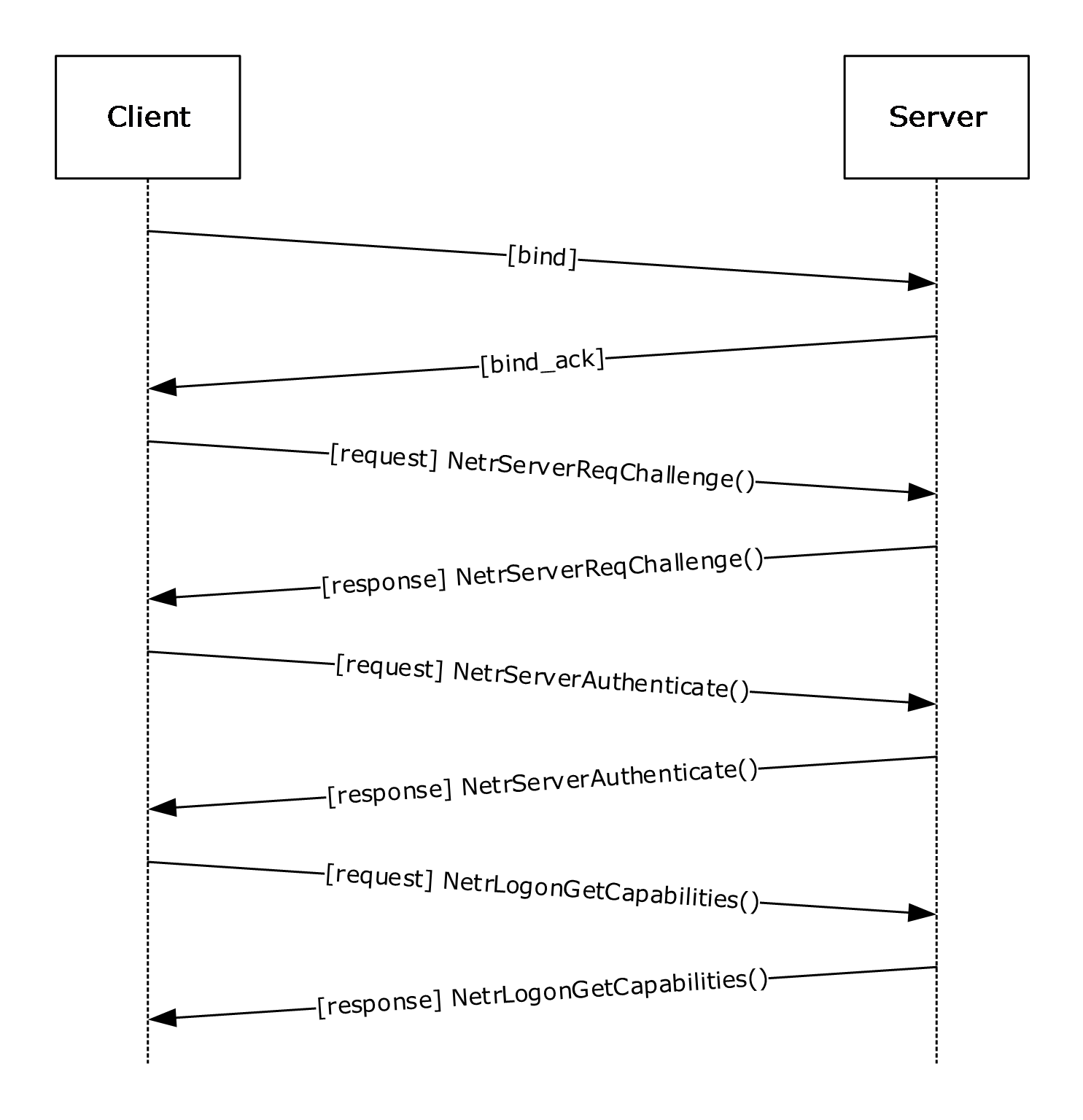


Figure 7: Session-key negotiation

Session-key negotiation works as follows.

1. The client binds to the remote Netlogon RPC [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee) on the server. The client then generates a [**nonce**](#gt_001c0e40-0980-417d-853c-f7cb34ba6d3b), called the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473), and sends the client challenge to the server as an input argument to the [NetrServerReqChallenge](#Section_5ad9db9f74414ce58c7b7b771e243d32) method call.
2. The server receives the client's NetrServerReqChallenge call. The server generates its own nonce, called the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9). In its response to the client's NetrServerReqChallenge method call, the server sends the SC back to the client as an output argument to NetrServerReqChallenge. After the client has received the server's response, both computers have one another's challenge nonce (client challenge and server challenge (SC), respectively).
3. The client computes a session key, as specified in section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63), Session-Key Computation. The client specifies an initial set of capabilities by providing an initial set of values in the NegotiateFlags.
4. The client computes its client Netlogon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) by using client challenge as input to the credential computation algorithm, as specified in section [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585).
5. The client exchanges its client Netlogon credential with the server by passing it in the [NetrServerAuthenticate](#Section_2561f16011f943a7bad45721a05e8ad8), [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355), or [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) call as the ClientCredential input argument. The selection of the particular method called by the client is specified in section [3.4.5.2.2](#Section_5ce4f403c16e42bc9c6e30d7e319feac).
6. The server receives the NetrServerAuthenticate, NetrServerAuthenticate2, or NetrServerAuthenticate3 call and verifies the client Netlogon credential. It does this by computing a session key, as specified in section 3.1.4.3, duplicating the client Netlogon credential computation, using its stored copy of client challenge, and comparing the result of this recomputation with the client Netlogon credential that was just received from the client. If the comparison fails, the server MUST fail session-key negotiation without further processing of the following steps.
7. The server computes its server Netlogon credential by using the server challenge as input to the credential computation algorithm, as specified in section 3.1.4.4. The server returns the server Netlogon credential as the ServerCredential output parameter of the NetrServerAuthenticate, NetrServerAuthenticate2, or NetrServerAuthenticate3 call.
8. The client verifies the server Netlogon credential. It does this by recomputing the server Netlogon credential, using its stored copy of server challenge, and comparing the result of this recomputation with the server Netlogon credential passed back from the server. If the comparison fails, the client MUST fail session-key negotiation.
9. Upon mutual verification, the client and server agree to use the computed session key for encrypting and/or signing further communications.
10. The client calls the NetrLogonGetCapabilities method (section [3.4.5.2.10](#Section_5e43f2088ecb4d10b5e5206836fe0e7d)).
11. The server SHOULD[<69>](#Appendix_A_69" \o "Product behavior note 69) return the negotiated flags for the current exchange.
12. The client SHOULD[<70>](#Appendix_A_70" \o "Product behavior note 70) compare the received ServerCapabilities (section [3.5.4.4.10](#Section_5780fc6c82f0489fb9a0a9e855388492)) with the negotiated NegotiateFlags (section 3.5.4.4.2), and if there is a difference, the session key negotiation is aborted.
13. The client sets the ServerSessionInfo.LastAuthenticationTry (indexed by server name) to the current time. This prevents authentication retries from occurring for 45 seconds, unless a new transport notification is received.

In the first phase of session-key negotiation (NetrServerReqChallenge), the client and server exchange nonces. This allows both the client and the server to compute a session key by using the algorithm described in section 3.1.4.3. To provide mutual authentication, both the client and the server calculate a Netlogon credential based on their own nonce, using the computed session key, and exchange them in the second phase of session-key negotiation (NetrServerAuthenticate or NetrServerAuthenticate2 or NetrServerAuthenticate3). Because nonces are exchanged in the first phase, this allows each side to calculate the other party's Netlogon credential locally, and then compare it with the received one. If the locally computed credential matches the one supplied by the other party, this proves to the client and to the server that the respective party has access to the [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1).

For more information about the methods involved in session-key negotiation, see client and server details in sections [3.4](#Section_2e745bde2f654857bd3c7de7b191c35a) and [3.5](#Section_1b79123d2f1e4970b9e8ea74ba95f95a).

#### Netlogon Negotiable Options

As part of the [**session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation, the client and server use the *NegotiateFlags* parameter of [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355) or [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) to negotiate support for the following options. The client offers an initial set of capabilities through the *NegotiateFlags* parameter to the server as input. The server then selects the capabilities acceptable to it. The capabilities that are supported by the server are combined with the capabilities supported by the client by performing a bit-wise AND; the result of the operation is returned to the client as output, as detailed in sections 3.5.4.4.2 and 3.5.4.4.3. The client MUST inspect the returned negotiation capabilities to determine whether server-selected capabilities are supported by the client, and that all of the capabilities required by the client are returned by the server. For example, a client could be configured outside the protocol to require strong-key support; if the server did not offer strong-key support, the client SHOULD reject the server.

If **NT4Emulator** is set to TRUE and bit U has not been set in *NegotiateFlags* as input, then the server MUST return 0 for bits J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, and Y in the output of the *NegotiateFlags* parameter.

The following options are negotiable between the client and the server as part of the session-key negotiation. An option is TRUE (or set) if its value is equal to 1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | Y | X | 0 | 0 | 0 | 0 | W | 0 | 0 | V | U | T | S | R | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | A |

Where the negotiable options SHOULD[<71>](#Appendix_A_71" \o "Product behavior note 71) be defined as the following:

| Option | Meaning |
| --- | --- |
| A | Not used. MUST be ignored on receipt. |
| B | Presence of this flag indicates that BDCs MAY[<72>](#Appendix_A_72" \o "Product behavior note 72) persistently try to update their [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) to the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d)'s version after they get a notification indicating that their database is out-of-date. Server-to-server only. |
| C | Supports [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) encryption. |
| D | Not used. MUST be ignored on receipt. |
| E | Supports BDCs handling CHANGELOGs. Server-to-server only. |
| F | Supports restarting of full synchronization between [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). Server-to-server only. |
| G | Does not require ValidationLevel 2 for nongeneric passthrough. |
| H | Supports the NetrDatabaseRedo (Opnum 17) functionality (section [3.5.4.6.4](#Section_c8352ce88b094baeaaf7456d7e6fda6c)). |
| I | Supports refusal of password changes. |
| J | Supports the NetrLogonSendToSam (Opnum 32) functionality. |
| K | Supports generic pass-through authentication. |
| L | Supports concurrent [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) calls. |
| M | Supports avoiding of user account database replication. Server-to-server only. |
| N | Supports avoiding of Security Authority database replication. Server-to-server only. |
| O | Supports strong keys. |
| P | Supports [**transitive trusts**](#gt_1c9fbb3f-ba87-419f-bd0c-39f73cee86f7). |
| Q | Not used. MUST be ignored on receipt. |
| R | Supports the [NetrServerPasswordSet2](#Section_14b020a80bcf4af5ab72cc92bc6b1d81) functionality. |
| S | Supports the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) functionality. |
| T | Supports cross-[**forest trusts**](#gt_035d9ce5-f117-4251-8d4d-127c462ec4a0). |
| U | Supports neutralizing Windows NT 4.0 operating system emulation. Note that when this flag is negotiated between a client and a server, it indicates that the server SHOULD ignore the **NT4Emulator** ADM element.[<73>](#Appendix_A_73" \o "Product behavior note 73) |
| V | Supports [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) pass-through to different [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).[<74>](#Appendix_A_74" \o "Product behavior note 74) |
| W | Supports [**Advanced Encryption Standard (AES)**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) encryption (128 bit in 8-bit CFB mode) and SHA2 hashing as specified in sections [2.2.1.3.3](#Section_fc77c8aa6c21446ba8224da26cc8a9a8), [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63), [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585), and [3.3](#Section_388e4b68f4e44e0498ecdfae7e9b1f01).[<75>](#Appendix_A_75" \o "Product behavior note 75) |
| X | Not used. MUST be ignored on receipt. |
| Y | Supports Secure RPC.[<76>](#Appendix_A_76" \o "Product behavior note 76) |

All other bits MUST be set as specified in the *NegotiateFlags* description and MUST be ignored on receipt.

#### Session-Key Computation

Although ClientChallenge and ServerChallenge are treated normally as byte arrays, ClientChallenge and ServerChallenge are treated as 64-bit integers in little-endian format to set the sum in the following pseudocode. The carry of the most-significant bit is ignored in the sum of the ClientChallenge and ServerChallenge.

##### AES Session-Key

If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) support is negotiated between the client and the server, the strong-key support flag is ignored and the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is computed with the HMAC-SHA256 algorithm [[RFC4634]](https://go.microsoft.com/fwlink/?LinkId=90486), as specified in the steps of pseudocode that follow. SHA256Reset, SHA256Input, SHA256FinalBits, and SHA256Result are predicates or functions specified in [RFC4634]. MD4 is specified in [[RFC1320]](https://go.microsoft.com/fwlink/?LinkId=90274).

1. ComputeSessionKey(SharedSecret, ClientChallenge,
2. ServerChallenge)
3. M4SS := MD4(UNICODE(SharedSecret))
4. CALL SHA256Reset(HashContext, M4SS, sizeof(M4SS));
5. CALL SHA256Input(HashContext, ClientChallenge, sizeof(ClientChallenge));
6. CALL SHA256FinalBits (HashContext, ServerChallenge, sizeof(ServerChallenge));
7. CALL SHA256Result(HashContext, SessionKey);
8. SET SessionKey to lower 16 bytes of the SessionKey;

The key produced with AES support negotiated is 128 bits (16 bytes).

##### Strong-key Session-Key

If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) is not negotiated and strong-key support is one of the flags in the NegotiateFlags between the client and the server, the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is computed with the MD5 message-digest algorithm [[RFC1321]](https://go.microsoft.com/fwlink/?LinkId=90275), as specified in the steps of pseudocode that follow. MD5Init, MD5Update, and MD5Final are predicates or functions specified in [RFC1321]. HMAC\_MD5 is a function specified in [[RFC2104]](https://go.microsoft.com/fwlink/?LinkId=90314). The md5Context variable is of type MD5\_CTX, as specified in [RFC1321].

1. SET zeroes to 4 bytes of 0
2. ComputeSessionKey(SharedSecret, ClientChallenge,
3. ServerChallenge)
4. M4SS := MD4(UNICODE(SharedSecret))
5. CALL MD5Init(md5context)
6. CALL MD5Update(md5context, zeroes, [4 bytes])
7. CALL MD5Update(md5context, ClientChallenge, [8 bytes])
8. CALL MD5Update(md5context, ServerChallenge, [8 bytes])
9. CALL MD5Final(md5context)
10. CALL HMAC\_MD5(md5context.digest, md5context.digest length,
11. M4SS, length of M4SS, output)
12. SET Session-Key to output

The key produced with strong-key support negotiated is 128 bits (16 bytes).

##### DES Session-Key

If neither [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) nor strong-key support is negotiated between the client and the server, the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is computed by using the DES encryption algorithm in ECB mode, as specified in [[FIPS81]](https://go.microsoft.com/fwlink/?LinkId=89874), as follows.

1. ComputeSessionKey(SharedSecret, ClientChallenge,
2. ServerChallenge)
3. M4SS := MD4(UNICODE(SharedSecret))
4. SET sum to ClientChallenge + ServerChallenge
5. SET k1 to lower 7 bytes of the M4SS
6. SET k2 to upper 7 bytes of the M4SS
7. CALL DES\_ECB(sum, k1, &output1)
8. CALL DES\_ECB(output1, k2, &output2)
9. SET Session-Key to output2

The key produced without AES and strong-key support negotiated is 64 bits and is padded to 128 bits with zeros in the most-significant bits.

#### Netlogon Credential Computation

When establishing a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca), the input is the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) when the Netlogon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) for the client is being computed, and the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9) when the Netlogon credential for the server is being computed. For subsequent calls using [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3), the input is the previously computed credential.

Output contains the computed 64-bit Netlogon credential.

##### AES Credential

If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) support is negotiated between the client and the server, the Netlogon [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) are computed using the AES-128 encryption algorithm in 8-bit CFB mode with a zero initialization vector.

1. ComputeNetlogonCredential(Input, Sk,
2. Output)
3. SET IV = 0
4. CALL AesEncrypt(Input, Sk, IV, Output)

AesEncrypt is the AES-128 encryption algorithm in 8-bit CFB mode with a zero initialization vector [[FIPS197]](https://go.microsoft.com/fwlink/?LinkId=89870).

##### DES Credential

The [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is computed as follows.

1. InitLMKey(KeyIn, KeyOut)
2. KeyOut[0] = KeyIn[0] >> 0x01;
3. KeyOut[1] = ((KeyIn[0]&0x01)<<6) | (KeyIn[1]>>2);
4. KeyOut[2] = ((KeyIn[1]&0x03)<<5) | (KeyIn[2]>>3);
5. KeyOut[3] = ((KeyIn[2]&0x07)<<4) | (KeyIn[3]>>4);
6. KeyOut[4] = ((KeyIn[3]&0x0F)<<3) | (KeyIn[4]>>5);
7. KeyOut[5] = ((KeyIn[4]&0x1F)<<2) | (KeyIn[5]>>6);
8. KeyOut[6] = ((KeyIn[5]&0x3F)<<1) | (KeyIn[6]>>7);
9. KeyOut[7] = KeyIn[6] & 0x7F;
10. for( int i=0; i<8; i++ ){
11. KeyOut[i] = (KeyOut[i] << 1) & 0xfe;
12. }

Assume bytes(s, e, l) returns bytes from s to e of the byte array l. After a session key is computed, a Netlogon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) is computed. If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) support is not negotiated between the client and the server, the Netlogon credentials are computed using DES:

1. ComputeNetlogonCredential(Input, Sk,
2. Output)
3. SET k1 to bytes(0, 6, Sk)
4. CALL InitLMKey(k1, k3)
5. SET k2 to bytes(7, 13, Sk)
6. CALL InitLMKey(k2, k4)
7. CALL DES\_ECB(Input, k3, &output1)
8. CALL DES\_ECB(output1, k4, &output2)
9. SET Output to output2

DES\_ECB is the DES encryption algorithm in ECB mode ([[FIPS81]](https://go.microsoft.com/fwlink/?LinkId=89874) and [[FIPS46-2]](https://go.microsoft.com/fwlink/?LinkId=89871)).

#### Netlogon Authenticator Computation and Verification

All methods that require a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca), except [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd), will use Netlogon [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3). If the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) call is using Netlogon authenticators, the following steps are used to calculate the authenticator:

1. Each time a client sends a new request, it records the current time stamp (expressed as the number of seconds since 00:00:00 on January 1, 1970 (UTC)) in the **TimeStamp** field of the [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5. The client also adds the value of this time stamp to the stored Netlogon client [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) and encrypts the result with the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d), using the Netlogon credential computation algorithm described in section [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585). The result of this computation is stored in the **Credential** field of the NETLOGON\_AUTHENTICATOR structure and is then sent to the server.
2. SET TimeNow = current time;
3. SET ClientAuthenticator.Timestamp = TimeNow;
4. SET ClientStoredCredential = ClientStoredCredential + TimeNow;
5. CALL ComputeNetlogonCredential(ClientStoredCredential,
6. Session-Key, ClientAuthenticator.Credential);
7. When the server receives a request, the server confirms the validity of the Netlogon authenticator that it received with the request. Validation is achieved by adding the time stamp transmitted in the received Netlogon authenticator to the server's stored copy of the Netlogon credential, and by encrypting the result with the session key, using the algorithm specified in section 3.1.4.4. The server then compares the Netlogon credential that it just calculated with the Netlogon credential transmitted in the received Netlogon authenticator. If the Netlogon credentials do not match, the operation fails, and an error indicating that access is denied is returned to the client.

If the Netlogon credentials match, the server increments the Netlogon credential in the Netlogon authenticator by one, performs the computation described in section 3.1.4.4, Netlogon Credential Computation, and stores the new Netlogon credential. The server returns a Netlogon authenticator that contains the new Netlogon credential to the client.

1. SET ServerStoredCredential = ServerStoredCredential +
2. ClientAuthenticator.Timestamp;
3. CALL ComputeNetlogonCredential(ServerStoredCredential,
4. Session-Key, TempCredential);
5. IF TempCredential != ClientAuthenticator.Credential
6. THEN return access denied error
7. SET ServerStoredCredential = ServerStoredCredential + 1;
8. CALL ComputeNetlogonCredential(ServerStoredCredential,
9. Session-Key, ServerAuthenticator.Credential);
10. The client validates the returned Netlogon authenticator by incrementing its stored Netlogon credential by one, encrypting the result with the session key using the algorithm described in section 3.1.4.4, and comparing the results. If this is successful, the client stores the Netlogon credential part of the Netlogon authenticator as the new Netlogon credential. If the validation failed, the client SHOULD re-establish its secure channel with the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).
11. SET ClientStoredCredential = ClientStoredCredential + 1;
12. CALL ComputeNetlogonCredential(ClientStoredCredential,
13. Session-Key, TempCredential);
14. IF TempCredential != ServerAuthenticator.Credential
15. THEN return abort

In each of the addition operations previously performed, the least-significant 4 bytes of the credential are added with the 4-byte time stamp value (or the constant 1), and overflow is ignored. This leaves the most-significant 4 bytes of the credential unmodified.

#### Calling Methods Requiring Session-Key Establishment

To call the methods in the following set, the client and the server MUST have performed [**session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation. If negotiation has not been completed prior to the time of a call, negotiation MUST be initiated and completed before making the call. Each method that requires a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is described in section [3.5](#Section_1b79123d2f1e4970b9e8ea74ba95f95a), with the errors specified. For descriptions of the following methods, see section 3.5.

* NetrGetForestTrustInformation
* NetrLogonGetCapabilities
* NetrLogonSamLogon
* NetrLogonSamLogonEx
* NetrLogonSamLogonWithFlags
* NetrLogonSamLogoff
* NetrLogonSendToSam
* NetrServerPasswordGet
* NetrServerPasswordSet
* NetrServerPasswordSet2
* NetrServerGetTrustInfo
* NetrServerTrustPasswordsGet
* NetrLogonGetDomainInfo
* NetrDatabaseDeltas
* NetrDatabaseSync2
* NetrDatabaseSync
* NetrDatabaseRedo
* NetrAccountDeltas
* NetrAccountSync
* NetrLogonDummyRoutine1

The client follows this sequence of steps.

1. The client binds to the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) server.[<77>](#Appendix_A_77" \o "Product behavior note 77)

The client and server SHOULD[<78>](#Appendix_A_78" \o "Product behavior note 78) utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.1.1.7) for privacy/integrity of the RPC messages. If the SealSecureChannel setting is TRUE, the client requests the Privacy [**authentication level**](#gt_bfb9708e-9d05-4f79-8969-ef63f73aa434) from the RPC runtime. If the SealSecureChannel setting is FALSE, then the authentication level requested is Integrity.

1. If the call to be made uses Netlogon [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3), the client MUST compute the Netlogon authenticator to be passed as a parameter to the RPC method, as specified in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).
2. The client calls the method on the server. If the RPC server denies access, the client SHOULD attempt to re-establish the session key with the target server if the difference between the current time and value of ServerSessionInfo.LastAuthenticationTry (indexed by the name of the target server) is greater than 45 seconds.
3. The server MUST verify the authenticator, if used, and compute the return authenticator, as specified in section 3.1.4.5.
4. The client MUST validate the returned authenticator, if used.
5. The client MAY unbind from the server, but it SHOULD[<79>](#Appendix_A_79" \o "Product behavior note 79) reuse the binding for multiple RPC calls.

#### Calling Methods Not Requiring Session-Key Establishment

The client follows this sequence of steps:

1. The client SHOULD bind to the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) server using the named pipe "\PIPE\NETLOGON", or MAY bind to the RPC server over TCP/IP.

**Note**  The TCP/IP channel cannot support impersonation for access control, and is therefore unusable. The server will ignore any calls made via this channel.

1. The client MUST call the method on the server.
2. The client SHOULD unbind from the server, or it MAY reuse the binding for multiple RPC calls.

#### Determining If the Implementation Is Running on a Domain Controller

The implementation determines whether it is running on a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) by querying the current server configuration by calling the abstract interface **ServerGetInfo** specified in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.6, specifying a level of 101. The resulting bufptr contains a **SERVER\_INFO\_101** structure, as specified in [MS-DTYP] section 2.3.12. The determination is TRUE if **sv101\_version\_type** contains SV\_TYPE\_DOMAIN\_CTRL or SV\_TYPE\_DOMAIN BAKCTRL. If **sv101\_version\_type** does not contain either of these values, the determination is FALSE.

#### Determining if a Request is for the Current Domain

If the server is running on a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the server determines if a request is for its [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) by comparing the domain the request was intended for and the domain-name ADM element.

#### Client Domain Controller Location

The client MUST attempt to locate a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) of a given [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). A client locally invokes processing rules specified in [DsrGetDCName](#Section_86a3fa5b1f0e412a942f33a10e5e9eff) (section 3.5.4.3.3) with the method parameters set as follows:

* Set the *ComputerName* parameter to NULL.
* Set the *DomainName* parameter to the [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c).
* Set the *DomainGuid* parameter to NULL.
* Set the *SiteGuid* parameter to NULL.
* Set the *Flags* parameter to a bitwise OR of the bits L and R that are specified in [DsrGetDcNameEx2](#Section_fb8e1146a0454c3198d1c68507ad5620) (section 3.5.4.3.1).

If DsrGetDCName returns with no errors, the **DomainControllerName** field of the returned **DomainControllerInfo** structure will contain the DC name.

### Timer Events

No protocol timer events are required on the client beyond the timers required in the underlying [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a).

### Other Local Events

No additional local events are used on the client beyond the events maintained in the underlying [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a) and Group Policy notification.

The Netlogon client and server register a local change notification callback with the Group Policy: Security Protocol Extension Client [[MS-GPSB]](%5bMS-GPSB%5d.pdf#Section_6a07a06be62847659d910d63ba47fdc0). The client SHOULD[<80>](#Appendix_A_80" \o "Product behavior note 80) send Netlogon a PolicyChange event when the policy is changed.

## Pass-Through Authentication Details

Netlogon has various roles, one of which is to securely transport data for authentication packages between the client and the server.

### Abstract Data Model

None.

### Timers

None.

### Initialization

Using Netlogon for pass-through authentication requires a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to have already been negotiated, as specified in section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9).

### Message Processing Events and Sequencing Rules

Netlogon is used to securely transport data for authentication packages between the client and the server. This is accomplished by packages calling the [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a) or [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd) methods. Netlogon takes the data specified in the input parameters by the authentication package on the client and sends it unexamined over the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to the server. The server delivers the data to the target authentication package.

#### Generic Pass-Through

When using the [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a) method, as specified in section 3.5.4.5.3, or the [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd) method, as specified in section 3.5.4.5.1, for generic pass-through, the following requirements MUST be met:

* The *LogonLevel* parameter is 4 ([NetlogonGenericInformation](#Section_8c7808e54e5c420e9c9047286da2218f)).
* The *ValidationLevel* parameter is 5 ([NetlogonValidationGenericInfo2](#Section_5eb0b7cb3a55477b92fcc236bd5873fa)).
* The *LogonInformation* parameter is [NETLOGON\_GENERIC\_INFO](#Section_c03d6d959b5e43299645eedcdd167f6e).
* NETLOGON\_GENERIC\_INFO.**PackageName** is "Kerberos" ([[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 3.2.5.1) or "WDigest" ([MS-APDS] section 3.3.5.1).

Protocols that use Netlogon for generic pass-through will also include opaque [**Binary Large Objects (BLOBs)**](#gt_ad861812-8cb0-497a-80bb-13c95aa4e425) that comprise their respective message data. These BLOBs are passed in the **LogonData** field of the NETLOGON\_GENERIC\_INFO structure, with the size of the data specified in the **DataLength** field. The BLOB is passed from one system's Netlogon component to the other system's component over the wire. Netlogon will then pass the opaque BLOB to the security package specified in the **PackageName** field.

The [NETLOGON\_LOGON\_IDENTITY\_INFO](#Section_81c44fa00a2741b3b607de39cce7ea1d) structure (as specified in section 2.2.1.4.15) inside the NETLOGON\_GENERIC\_INFO structure (as specified in section 2.2.1.4.2) MUST:

* Contain the LogonDomainName.
* Ensure that the rest of the NETLOGON\_LOGON\_IDENTITY\_INFO fields are zeroed out.

The response is sent by the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) via the *ValidationInformation* parameter, which points to a pointer to the [NETLOGON\_VALIDATION\_GENERIC\_INFO2](#Section_e89f8f5b098541a0b1101ae0ea2bd183) structure.

See [MS-APDS] for a specification of how NTLM, Kerberos, and Digest authentication packages use the Netlogon [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca).

### Timer Events

No protocol timer events are required on the client beyond the timers required in the underlying [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a).

### Other Local Events

No additional local events are used on the client beyond the events maintained in the underlying [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a).

## Netlogon as a Security Support Provider

In addition to other functionality, Netlogon also serves as a limited private SSP[<81>](#Appendix_A_81" \o "Product behavior note 81) for use by Netlogon and [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.1.1.7) when encrypting and signing data during communication.[<82>](#Appendix_A_82" \o "Product behavior note 82) Central to this capability is the use of the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d), as specified in section [3.1](#Section_273b6905782d4a7ea2e44337816916e0). This section specifies the behavior of the [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) role for both client and server.

Netlogon implements a service that allows the RPC runtime to perform a [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) negotiation between the client and the server and to use per-message calls to protect the data being passed over the network. For Netlogon to be able to perform this functionality, a session key

MUST have been established between the client and the server as described in section 3.1. Netlogon registers with the RPC runtime as a security provider with the auth\_type value (as specified in [MS-RPCE] section 2.2.2.11) of 0x44.

When serving as its own generic SSP, Netlogon always provides the following service features:

* Integrity: Signed messages are constructed so that they cannot be tampered with while in transit. The generation and receipt of the [Netlogon Signature](#Section_2af2dc5f794143aba6d063161a591a6e) token will always provide integrity protection for the messages.
* Sequence Detect: Signed messages are constructed such that out-of-order sequences can be detected. The generation and receipt of the Netlogon Signature token will always detect out-of-sequence messages.

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

Netlogon serves as a [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) for its own [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) connections. As such, it provides the following service: Confidentiality.

For protocol features, once a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) has been established through the session-key negotiation, Netlogon relies upon the RPC runtime to invoke the per-message functions. The following define the services provided by the Netlogon [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a).

**Note**  The following defined variables are logical, abstract parameters that an implementation is required to maintain and expose to provide the proper level of service. How these variables are maintained and exposed is determined by the implementation.

**Confidentiality:**  A Boolean setting that indicates that the caller is requiring encryption of messages so that they cannot be read while in transit. Requesting this service results in Netlogon encrypting the message. For more information, see sections [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed) and [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63).

As per [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.2.11, the **auth\_level** field of the **sec\_trailer** structure determines the [**authentication level**](#gt_bfb9708e-9d05-4f79-8969-ef63f73aa434) used. Netlogon only supports RPC\_C\_AUTHN\_LEVEL\_PKT\_INTEGRITY and RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY. A value of RPC\_C\_AUTHN\_LEVEL\_PKT\_INTEGRITY implies that Integrity is provided by the Netlogon SSP, and a value of RPC\_C\_AUTHN\_LEVEL\_PKT\_PRIVACY implies that Confidentiality is provided by the Netlogon SSP. Sequence detection is always provided.

The Netlogon SSP maintains the following set of data for each session:

**ClientSequenceNumber:** A 64-bit integer value used for detecting out-of-order messages on the client side.

**ServerSequenceNumber:** A 64-bit integer value used for detecting out-of-order messages on the server side.

**Session-Key:** See section 3.1.4.3 for **Session-Key** computation details.

**NegotiateFlags:** See section [3.1.1](#Section_708b71329e72447c992bd0bef4078f81) for **NegotiateFlags** details.

**MessageBlockSize:** An integer that indicates the minimum size of messages for encryption. This value MUST be 1.

### Timers

None.

### Initialization

Establishing a Netlogon [**security context**](#gt_88d49f20-6c95-4b64-a52c-c3eca2fe5709) requires a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to have already been negotiated, as described in section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9).

### Message Processing Events and Sequencing Rules

Netlogon uses two types of tokens when functioning as an SSP: [NL\_AUTH\_MESSAGE](#Section_525f0bf3ebd943609343685767eb3c67) and [NL\_AUTH\_SIGNATURE](#Section_05b99afd1b6a4207b16e959e6a483867).

#### The NL\_AUTH\_MESSAGE Token

The NL\_AUTH\_MESSAGE token contains information that is part of the first message in an authenticated transaction between a client and a server. It contains a message type, flags, and naming information. For the exact format, see section [2.2.1.3.1](#Section_525f0bf3ebd943609343685767eb3c67).

The NL\_AUTH\_MESSAGE token is part of the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) PDU AUTH trailer structure as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 2.2.2.11.

The client generates an initial token and sends it to the server. The server receives the token, processes it, and passes back a return token to the client.

The exchange of this message requires a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to have been negotiated as described in section [3.1](#Section_273b6905782d4a7ea2e44337816916e0). Upon successful exchange of tokens, the application can start using per-message calls to protect the data being passed over the network.

##### Generating an Initial NL\_AUTH\_MESSAGE Token

The client generates a [NL\_AUTH\_MESSAGE token](#Section_b28a01cb295d4833bdb6b113baf109b4) to initiate authentication to a server. The **MessageType** field of this token MUST be set to zero to indicate that this is a Negotiate message type.

The client MUST provide at least one [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) and one [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b) in the token by providing the **Flags** bit and the corresponding text buffer. The **Flags** field is a bitwise OR of the values described under the **Flags** field of the NL\_AUTH\_MESSAGE token in section [2.2.1.3.1](#Section_525f0bf3ebd943609343685767eb3c67). This value represents the names available in the token. The **Buffer** field is then composed by concatenating the strings of the names indicated by the **Flags** value. The compressed UTF-8 strings are generated, as specified in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) section 4.1.4.

The following is an example token on the wire.

1. 00 00 00 00 17 00 00 00 4E 54 44 45 56 00 4E 41 ........NTDEV.NA
2. 53 4B 4F 00 05 6E 74 64 65 76 04 63 6F 72 70 09 SKO..ntdev.corp.
3. 6D 69 63 72 6F 73 6F 66 74 03 63 6F 6D 00 05 4E microsoft.com..N
4. 41 53 4B 4F 00 ASKO.

##### Receiving an Initial NL\_AUTH\_MESSAGE Token

When the server receives the initial NL\_AUTH\_MESSAGE token, the server will check the token type and extract the client names using the Flags values and corresponding text buffer passed. The server MUST return SEC\_E\_INVALID\_TOKEN (0x80090308), indicating that an invalid token has been received, when any of the following are true:

* The MessageType is not set to 0x00000000.
* A flag for a particular name type is present and the corresponding text buffer cannot be extracted from the Buffer.
* The token does not contain at least one [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) and one [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b).

The server initializes **ServerSequenceNumber** to 0. This sequence number is used to detect out-of-order messages.

##### Generating a Return NL\_AUTH\_MESSAGE Token

Upon successful verification and extraction of data from the initial token, the server verifies that a successful [**session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation has occurred by the presence of the **Session-Key** data item for the client. If no negotiation has occurred, the server MUST return SEC\_E\_INVALID\_TOKEN (0x80090308) indicating that an invalid token has been received.

The server generates a return NL\_AUTH\_MESSAGE (section [2.2.1.3.1](#Section_525f0bf3ebd943609343685767eb3c67)) token. The **MessageType** MUST be set to 1 to indicate that this is a Negotiate response message type, the **Flags** field SHOULD be set to zero, the **Buffer** field SHOULD contain a NULL character, and the NL\_AUTH\_MESSAGE token MUST be padded to 12 bytes in length.

The return NL\_AUTH\_MESSAGE token is then sent back to the client along with any additional application-specific data.

##### Receiving a Return NL\_AUTH\_MESSAGE Token

When the client receives the return token, it verifies that:

* the NL\_AUTH\_MESSAGE token is at least 12 bytes in length, and
* the MessageType is set to 1.

If either of these conditions are not true, the client MUST return SEC\_E\_INVALID\_TOKEN (0x80090308) indicating that an invalid token has been received.

Otherwise, the client initializes ClientSequenceNumber to 0, which is used to detect out-of-order messages.

#### The Netlogon Signature Token

The Netlogon Signature token contains information that MUST be part of each protected message. It contains a signature algorithm identifier, encryption algorithm identifier, confounder, flags, sequence number, and checksum (see section [2.2.1.3.2](#Section_05b99afd1b6a4207b16e959e6a483867) for the exact format). When data is protected/signed, a Netlogon Signature token is generated that describes the algorithms used and contains the checksum of the data to be sent. When data is received and is unprotected/verified, the Netlogon Signature token is used.

##### Generating a Client Netlogon Signature Token

If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) is negotiated, a client generates an [NL\_AUTH\_SHA2\_SIGNATURE](#Section_fc77c8aa6c21446ba8224da26cc8a9a8) token that contains an HMAC-SHA256 checksum [[RFC4634]](https://go.microsoft.com/fwlink/?LinkId=90486), a sequence number, and a **Confounder** (if confidentiality has been requested) to send data protected on the wire. The data is encrypted using the AES algorithm. If AES is not negotiated, a client generates a [Netlogon Signature token](#Section_2af2dc5f794143aba6d063161a591a6e) that contains an [**HMAC-MD5**](#gt_ba024019-a866-41df-99a5-764b7eab2e1e) checksum ([[RFC2104]](https://go.microsoft.com/fwlink/?LinkId=90314)), a sequence number, and a **Confounder** (if confidentiality has been requested) to send data protected on the wire. The data is encrypted using the negotiated encryption algorithm. Note that in the algorithm that follows, the term Confidentiality is used as defined in section [3.3.1](#Section_a7bd20030d614686aa6e89336cec83a1). The following steps are performed to generate the client Netlogon Signature tokens and to encrypt the data if requested.

1. If AES is negotiated:
   * The **SignatureAlgorithm** first byte MUST be set to 0x13, and the second byte MUST be set to 0x00.
   * If the Confidentiality option (section 3.3.1) is requested from the application, then the **SealAlgorithm** first byte MUST be set to 0x1A, the second byte MUST be set to 0x00, and the **Confounder** MUST be filled with cryptographically random data.
   * If the Confidentiality option (section 3.3.1) is not requested, then the **SealAlgorithm** MUST be filled with two bytes of 0xff and the **Confounder** is not included in the token.
2. If AES is not negotiated:
   * The **SignatureAlgorithm** first byte MUST be set to 0x77, and the second byte MUST be set to 0x00.
   * If the Confidentiality option (section 3.3.1) is requested from the application, then the **SealAlgorithm** first byte MUST be set to 0x7A, the second byte MUST be set to 0x00, and the **Confounder** MUST be filled with cryptographically random data.
   * If the Confidentiality option is not requested, then the **SealAlgorithm** MUST be filled with two bytes of value 0xff and the **Confounder** is not included in the token.
3. The **Pad** MUST be filled with 0xff bytes.
4. The **Flags** MUST be filled with 0x00 bytes.
5. The **SequenceNumber** MUST be computed using the following algorithm.
6. Assume byte(n, l) returns byte n of the 32-bit number l.
7. The n parameter is limited to 0..3. The least significant
8. byte is 0, the most significant byte is 3.
9. SET CopySeqNumber[0] to byte(3, ClientSequenceNumber.LowPart)
10. SET CopySeqNumber[1] to byte(2, ClientSequenceNumber.LowPart)
11. SET CopySeqNumber[2] to byte(1, ClientSequenceNumber.LowPart)
12. SET CopySeqNumber[3] to byte(0, ClientSequenceNumber.LowPart)
13. SET CopySeqNumber[4] to byte(3, ClientSequenceNumber.HighPart)
14. SET CopySeqNumber[5] to byte(2, ClientSequenceNumber.HighPart)
15. SET CopySeqNumber[6] to byte(1, ClientSequenceNumber.HighPart)
16. SET CopySeqNumber[7] to byte(0, ClientSequenceNumber.HighPart)
17. Set CopySeqNumber[4] to CopySeqNumber[4] OR 0x80
18. The **ClientSequenceNumber** MUST be incremented by 1.
19. If AES is negotiated, then a signature MUST be computed using the following algorithm:
20. CALL SHA256Reset(&HashContext, Sk, sizeof(Sk));
21. CALL SHA256Input(HashContext, NL\_AUTH\_SHA2\_SIGNATURE, [8 bytes]);
22. IF Confidentiality requested
23. CALL SHA256Input(HashContext, Confounder, [8 bytes]);
24. CALL SHA256FinalBits(HashContext, Message, size of Message;
25. CALL SHA256Result(HashContext, output);
26. SET Signature to output
27. Note: In the first call to SHA256Input, only the first 8-bytes
28. of the NL\_AUTH\_SHA2\_SIGNATURE structure are used.

Else, a signature MUST be computed using the following algorithm:

1. SET zeroes to 4 bytes of 0
2. CALL MD5Init(md5context)
3. CALL MD5Update(md5context, zeroes, [4 bytes])
4. CALL MD5Update(md5context, NL\_AUTH\_SIGNATURE, [8 bytes])
5. IF Confidentiality requested
6. CALL MD5Update(md5context, Confounder, [8 bytes])
7. CALL MD5Update(md5context, Message, size of Message)
8. CALL MD5Final(md5context)
9. CALL HMAC\_MD5(md5context.digest, md5context.digest length,
10. Session-Key, size of Session Key, output)
11. SET Signature to output
12. Note: In the second call to MD5Update, only the first 8-bytes
13. of the NL\_AUTH\_SIGNATURE structure are used.

After the signature is computed, the signature MUST be truncated, with only the first 8 bytes being copied into the **Checksum** field of [NL\_AUTH\_SIGNATURE](#Section_05b99afd1b6a4207b16e959e6a483867).

1. If the Confidentiality option is requested, the **Confounder** field and the data MUST be encrypted, in that order, using the same encryption algorithm.
   * If AES is negotiated, then the server MUST use AES-128 for encryption. The server MUST derive the AES key using the following algorithm:
2. FOR (I=0; I < Key Length; I++)
3. EncryptionKey[I] = SessionKey[I] XOR 0xf0

The server MUST encrypt the **Confounder** field using the initialization vector constructed by concatenating the sequence number with itself twice (thus getting 16 bytes of data). For encrypting the data, the initialization vector MUST be constructed using the last block of the encrypted **Confounder** field.

* + Else, the server MUST use [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) for encryption. The server MUST derive the RC4 key using the following algorithm:

1. SET zeroes to 4 bytes of 0
2. FOR (I=0; I < Key Length; I++)
3. XorKey [I] = SessionKey[I] XOR 0xf0
4. CALL hmac\_md5(zeroes, [4 bytes], XorKey, size of XorKey, TmpData)
5. CALL hmac\_md5(CopySeqNumber, size of CopySeqNumber, TmpData,
6. size of TmpData, EncryptionKey)

The hmac\_md5 function is defined in the Appendix of [RFC2104]. The server MUST use this key to initialize RC4 and encrypt the **Confounder** field and then the data. The server MUST initialize RC4 only once, before encrypting the **Confounder** field.

1. The **SequenceNumber** MUST be encrypted. If AES is negotiated, then the AES-128 algorithm MUST be used, using the SessionKey with an initialization vector constructed by concatenating the first 8 bytes of the checksum with itself twice (thus getting 16 bytes of data), otherwise the RC4 algorithm MUST be used.

The RC4 key MUST be derived as follows:

1. SET zeroes to 4 bytes of 0
2. CALL hmac\_md5(zeroes, [4 bytes], SessionKey, size of SessionKey, TmpData)
3. CALL hmac\_md5(Checksum, size of Checksum, TmpData, size of TmpData,
4. EncryptionKey)

The NetLogon Signature token MUST then be sent to the server along with the data.

##### Receiving a Client Netlogon Signature Token

When a server receives encrypted data, it verifies the [Netlogon Signature](#Section_2af2dc5f794143aba6d063161a591a6e) token. If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) is negotiated, a server receives an [NL\_AUTH\_SHA2\_SIGNATURE](#Section_fc77c8aa6c21446ba8224da26cc8a9a8) structure, otherwise it receives an [NL\_AUTH\_SIGNATURE](#Section_05b99afd1b6a4207b16e959e6a483867) structure. The following steps are performed to verify the data and to decrypt with AES if negotiated, otherwise [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) if required:

1. The **SignatureAlgorithm** bytes MUST be verified to ensure:
   * If AES is negotiated, the first byte is set to 0x13; otherwise the first byte is set to 0x77.
   * The second byte is set to 0x00.

If either of these two is incorrect, an SEC\_E\_MESSAGE\_ALTERED (0x8009030F) MUST be returned.

1. If the Confidentiality option is requested from the application, then the **SealAlgorithm** MUST be verified to ensure that if AES is negotiated, the first byte is set to 0x1A; otherwise the first byte is set to 0x7A. The second byte is set to 0x00.

If the Confidentiality option is not requested, then the **SealAlgorithm** MUST be verified to contain all 0xff bytes.

If either of these two is incorrect, an SEC\_E\_MESSAGE\_ALTERED (0x8009030F) MUST be returned.

1. The **Pad** MUST be verified to contain all 0xff bytes and SEC\_E\_MESSAGE\_ALTERED (0x8009030F) MUST be returned otherwise.
2. The **Flags** data SHOULD be[<83>](#Appendix_A_83" \o "Product behavior note 83) disregarded.
3. The **SequenceNumber** MUST be decrypted. If AES is negotiated, then the AES-128 algorithm MUST be used with Session Key and an initialization vector constructed by concatenating the checksum with itself (thus getting 16 bytes of data). Otherwise, the RC4 algorithm MUST be used. The RC4 key MUST be derived as follows:
4. SET zeroes to 4 bytes of 0
5. CALL hmac\_md5(zeroes, [4 bytes], SessionKey, size of SessionKey, TmpData)
6. CALL hmac\_md5(Checksum, size of Checksum, TmpData, size of TmpData,
7. DecryptionKey)
8. A local copy of **SequenceNumber** MUST be computed using the following algorithm.
9. Assume byte(n, l) returns byte n of the 32-bit number l. The n
10. parameter is limited to 0..3. The least significant byte is 0,
11. the most significant byte is 3.
12. SET CopySeqNumber[0] to byte(3, ServerSequenceNumber.LowPart)
13. SET CopySeqNumber[1] to byte(2, ServerSequenceNumber.LowPart)
14. SET CopySeqNumber[2] to byte(1, ServerSequenceNumber.LowPart)
15. SET CopySeqNumber[3] to byte(0, ServerSequenceNumber.LowPart)
16. SET CopySeqNumber[4] to byte(3, ServerSequenceNumber.HighPart)
17. SET CopySeqNumber[5] to byte(2, ServerSequenceNumber.HighPart)
18. SET CopySeqNumber[6] to byte(1, ServerSequenceNumber.HighPart)
19. SET CopySeqNumber[7] to byte(0, ServerSequenceNumber.HighPart)
20. Set CopySeqNumber[4] to CopySeqNumber[4] OR 0x80
21. The **SequenceNumber** MUST be compared to **CopySeqNumber**. If these two do not match, SEC\_E\_OUT\_OF\_SEQUENCE MUST be returned.
22. **ServerSequenceNumber** MUST be incremented.

If the Confidentiality option is requested, the **Confounder** and the data MUST be decrypted using RC4.

1. If the Confidentiality option is requested, the **Confounder** and the data MUST be decrypted.
   * The AES key used MUST be derived using the following algorithm:
2. FOR (I=0; I < Key Length; I++)
3. EncryptionKey [I] = SessionKey[I] XOR 0xf0

If AES is negotiated, decrypt using an initialization vector constructed by concatenating twice the sequence number (thus getting 16 bytes of data).

* + The RC4 key used MUST be derived using the following algorithm:

1. SET zeroes to 4 bytes of 0
2. FOR (I=0; I < Key Length; I++)
3. XorKey [I] = SessionKey[I] XOR 0xf0
4. CALL hmac\_md5(zeroes, [4 bytes], XorKey, size of XorKey, TmpData)
5. CALL hmac\_md5(CopySeqNumber, size of CopySeqNumber, TmpData,
6. size of TmpData, EncryptionKey)

The hmac\_md5 function is specified in [[RFC2104]](https://go.microsoft.com/fwlink/?LinkId=90314).

1. If AES is negotiated, then a signature MUST be computed using the following algorithm:
2. CALL SHA256Reset(&HashContext, Sk, sizeof(Sk));
3. CALL SHA256Input(HashContext, NL\_AUTH\_SHA2\_SIGNATURE, [8 bytes]);
4. IF Confidentiality requested
5. CALL SHA256Input(HashContext, Confounder, [8 bytes]);
6. CALL SHA256FinalBits(HashContext, Message, size of Message);
7. CALL SHA256Result(HashContext, output);
8. SET Signature to output
9. Note: In the first call to SHA256Input only the first 8-bytes
10. of the NL\_AUTH\_SHA2\_SIGNATURE structure are used.

Else a signature MUST be computed using the following algorithm:

1. SET zeroes to 4 bytes of 0
2. CALL MD5Init(md5context)
3. CALL MD5Update(md5context, zeroes, [4 bytes])
4. CALL MD5Update(md5context, NL\_AUTH\_SIGNATURE, [8 bytes])
5. IF Confidentiality requested
6. CALL MD5Update(md5context, Confounder, [8 bytes])
7. CALL MD5Update(md5context, Message, size of Message)
8. CALL MD5Final(md5context)
9. CALL HMAC\_MD5(md5context.digest, md5context.digest length,
10. Session Key, size of Session Key, output)
11. SET Signature to output
12. Note: In the second call to MD5Update only the first 8-bytes
13. of the NL\_AUTH\_SIGNATURE structure are used.
14. The first 8 bytes of the computed signature MUST be compared to the checksum. If these two do not match, the SEC\_E\_MESSAGE\_ALTERED (0x8009030F) MUST be returned, indicating that the message was altered.

##### Generating a Server Netlogon Signature Token

If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) is negotiated, a server generates an [NL\_AUTH\_SHA2\_SIGNATURE](#Section_fc77c8aa6c21446ba8224da26cc8a9a8) token that contains an HMAC-SHA256 checksum [[RFC4634]](https://go.microsoft.com/fwlink/?LinkId=90486), a sequence number, and a **Confounder** (if confidentiality has been requested) to send data protected on the wire. The data is encrypted using the AES algorithm. If AES is not negotiated, a client generates a [Netlogon Signature](#Section_2af2dc5f794143aba6d063161a591a6e) token that contains an [**HMAC-MD5**](#gt_ba024019-a866-41df-99a5-764b7eab2e1e) checksum ([[RFC2104]](https://go.microsoft.com/fwlink/?LinkId=90314)), a sequence number, and a **Confounder** (if confidentiality has been requested) to send data protected on the wire. The data is encrypted using the negotiated encryption algorithm. Note that in the algorithm that follows, the term Confidentiality is used as defined in section [3.3.1](#Section_a7bd20030d614686aa6e89336cec83a1). The following steps are performed to generate the server Netlogon Signature tokens and to encrypt the data if requested.

1-4. Same as steps 1-4 in section [3.3.4.2.1](#Section_0593a87c7a83423280f8571e34220fed).

5. The **SequenceNumber** MUST be computed using the following algorithm:

1. Assume byte(n, l) returns byte n of the 32-bit number l.
2. The n parameter is limited to 0..3. The least significant
3. byte is 0, the most significant byte is 3.
4. SET CopySeqNumber[0] to byte(3, ServerSequenceNumber.LowPart)
5. SET CopySeqNumber[1] to byte(2, ServerSequenceNumber.LowPart)
6. SET CopySeqNumber[2] to byte(1, ServerSequenceNumber.LowPart)
7. SET CopySeqNumber[3] to byte(0, ServerSequenceNumber.LowPart)
8. SET CopySeqNumber[4] to byte(3, ServerSequenceNumber.HighPart)
9. SET CopySeqNumber[5] to byte(2, ServerSequenceNumber.HighPart)
10. SET CopySeqNumber[6] to byte(1, ServerSequenceNumber.HighPart)
11. SET CopySeqNumber[7] to byte(0, ServerSequenceNumber.HighPart)

6. The **ServerSequenceNumber** MUST be incremented by one. The Netlogon Signature token MUST then be sent to the client along with the data.

7-9. Same as steps 7-9 in section 3.3.4.2.1.

##### Receiving a Server Netlogon Signature Token

When a client receives encrypted data, it verifies the [Netlogon Signature](#Section_2af2dc5f794143aba6d063161a591a6e) token. If [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) is negotiated, a client receives an [NL\_AUTH\_SHA2\_SIGNATURE](#Section_fc77c8aa6c21446ba8224da26cc8a9a8) structure, otherwise it receives an [NL\_AUTH\_SIGNATURE](#Section_05b99afd1b6a4207b16e959e6a483867) structure. The following steps are performed to verify the data and to decrypt with AES if negotiated, otherwise [**RC4**](#gt_d57eac33-f561-4a08-b148-dfcf29cfb4d8) MUST be used if required.

1-5. Same as steps 1-5 in section [3.3.4.2.2](#Section_4daf7de2197f48eab34cea71773fde9b).

6. A local copy of **SequenceNumber** MUST be computed using the following algorithm.

1. Assume byte(n, l) returns byte n of the 32-bit number l. The n
2. parameter is limited to 0..3. The least significant byte is 0,
3. the most significant byte is 3.
4. SET CopySeqNumber[0] to byte(3, ClientSequenceNumber.LowPart)
5. SET CopySeqNumber[1] to byte(2, ClientSequenceNumber.LowPart)
6. SET CopySeqNumber[2] to byte(1, ClientSequenceNumber.LowPart)
7. SET CopySeqNumber[3] to byte(0, ClientSequenceNumber.LowPart)
8. SET CopySeqNumber[4] to byte(3, ClientSequenceNumber.HighPart)
9. SET CopySeqNumber[5] to byte(2, ClientSequenceNumber.HighPart)
10. SET CopySeqNumber[6] to byte(1, ClientSequenceNumber.HighPart)
11. SET CopySeqNumber[7] to byte(0, ClientSequenceNumber.HighPart)

7. Same as step 7 in section 3.3.4.2.2.

8. **ClientSequenceNumber** MUST be incremented.

9-11. Same as steps 9-11 in section 3.3.4.2.2.

### Timer Events

None.

### Other Local Events

None.

## Netlogon Client Details

The following sections specify data and state maintained by the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) client. They include details of calling Netlogon RPC methods on the client side of the client/server communication. A client in this context can be a [**domain member (member machine)**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65), a member server, or a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). The provided data is to facilitate the explanation of how the protocol behaves. This section does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.[<84>](#Appendix_A_84" \o "Product behavior note 84)

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

The Netlogon Protocol client maintains the following variables in addition to the ones described in section [3.1](#Section_273b6905782d4a7ea2e44337816916e0), Netlogon Common Details, which are part of the abstract state.

**ClientCapabilities:** A 32-bit set of flags defined in section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed) that identify the client's supported options.

**domain-name (Public):** For client machines, the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) to which the machine has been joined. This ADM element is shared with **DomainName.NetBIOS** ([[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) section 3.2.1.6). For [**domain controllers**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) to which the domain controller has a [**direct trust**](#gt_e03f25c6-dd6e-43df-83e2-98f89bcc50d9).

The Netlogon client variables that are registry keys are as follows:

**RejectMD5Servers:** A Boolean variable that indicates whether the client SHOULD[<85>](#Appendix_A_85" \o "Product behavior note 85) reject servers that are using MD5 encryption.

**RequireSignOrSeal:** Indicates whether the client SHOULD[<86>](#Appendix_A_86" \o "Product behavior note 86) continue session-key negotiation when the server did not specify support for Secure [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) as described in the negotiable option Y of section 3.1.4.2.

**RequireStrongKey:** A Boolean variable that indicates whether the client SHOULD[<87>](#Appendix_A_87" \o "Product behavior note 87)[<88>](#Appendix_A_88" \o "Product behavior note 88) negotiate the use of a strong key during [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) creation as described by the negotiable option O of section 3.1.4.2.

These registry keys and values MUST be exposed at a specified registry path via the Windows Remote Registry Protocol [[MS-RRP]](%5bMS-RRP%5d.pdf#Section_0fa3191dbb79490a81bd54c2601b7a78). For each abstract data model (ADM) element that is loaded from the registry, there is one instance that is shared between the Windows Remote Registry Protocol and the protocol(s) that uses the ADM element. Any changes made to the **RejectMD5Servers** registry key will not be reflected in the ADM elements until the Netlogon server is stopped and restarted. Any changes made to the **RequireStrongKey** and **RequireSignOrSeal** registry keys are reflected in the ADM elements when a PolicyChange event is received (section 3.1.6).

When a secure channel is established, the client maintains:

**ServerSessionInfo**: A table indexed by *PrimaryName* with the following members:

* **PrimaryName**: The *PrimaryName* (section [3.5.4.4.1](#Section_5ad9db9f74414ce58c7b7b771e243d32)) used by the client during session-key negotiations (section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9)).
* **ClientSequenceNumber**: See section [3.3.1](#Section_a7bd20030d614686aa6e89336cec83a1) for *ClientSequenceNumber* details.
* **ServerSequenceNumber**: See section 3.3.1 for *ServerSequenceNumber* details.
* **Session-Key**: See section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63) for *Session-Key* computation details.
* **NegotiateFlags**: See section [3.1.1](#Section_708b71329e72447c992bd0bef4078f81) for *NegotiateFlags* details.
* **ClientStoredCredential**: See section 3.1.1 for *ClientStoredCredential* details.
* **DomainName**: See section 3.1.1 for *ClientStoredCredential* details.
* **ConnectionStatus**: See section 3.1.1 for *ClientStoredCredential* details.
* **LastAuthenticationTry**: A FILETIME ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.3.3) indicating the time when the last authentication attempt was made. The time stamp is used to determine if at least 45 seconds have passed since the last authentication attempt.

### Timers

If the client is running on a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the client MUST create a domainControllerCacheTimer with an expiry of 15 minutes. The operation of this timer is specified in section [3.4.6.1](#Section_35a7b9edf2e44953b25e569a62fe62df).

### Initialization

If the client is running on a member workstation, the client MUST initialize the **LocatedDCsCache** with one entry, as follows:

* The client MUST attempt to locate a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) from the client's [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) by performing the steps described in section [3.1.4.10](#Section_00ac739d274d434b9efbfad10405721a) for the domain specified by the domain-name ADM element. If a DC is successfully located, the **LocatedDCsCache** is populated based on the resulting DomainControllerInfo structure.
* If the client fails to locate a DC, the client ignores errors and MUST continue initialization.

If the client is running on a DC, the client MUST initialize the **LocatedDCsCache** for each domain [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) by the client DC, as follows:

* The client MUST get a trusted domain list by performing the external behavior consistent with locally invoking LsarEnumerateTrustedDomains ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.8).
  + The *EnumerationContext* parameter MUST be set to 0.
  + The *PreferredMaximumLength* SHOULD[<89>](#Appendix_A_89" \o "Product behavior note 89) be set to 4096.
  + A policy handle is not needed locally.
* The client MUST attempt to locate a DC (section 3.1.4.10) for each of the domain entries of the returned trusted domain list.
  + If the client fails when attempting to locate a DC for a domain entry in the trusted domain list, the client MUST ignore errors and continue to attempt to locate DCs for the remaining domain entries in the trusted domain list.
  + For each successfully located DC, the client must add an entry to the ServerSessionInfo table with the new entry's **PrimaryName** set to **DOMAIN\_CONTROLLER\_INFOW.DomainControllerName** and the new entry's **DomainName** set to **DOMAIN\_CONTROLLER\_INFOW.DomainName**.
* For each located DC, the client MUST attempt to establish a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) with the located DC (section 3.1.4.10)

**ServerSessionInfo** MUST be empty.

**ClientCapabilities** SHOULD be initialized in an implementation-specific way to reflect the capabilities offered by that client implementation. The client SHOULD set the value according to the bit field, defined as shown in Netlogon Negotiable Options (section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed)). Bits C, G, I, J, K, L, O, P, R, S, T, V, W, and Y SHOULD[<90>](#Appendix_A_90" \o "Product behavior note 90) be set to 1 when a corresponding capability is supported by a given implementation. Bit U SHOULD be set if the client is determined to be running on a domain controller (section [3.1.4.8](#Section_16f8294280d643ac8c38eee3cfe4ac99)). Other bits are not used and MAY be set to zero, but will be ignored upon receipt.

**RejectMD5Servers** MUST be initialized to FALSE.

**RequireSignOrSeal** SHOULD[<91>](#Appendix_A_91" \o "Product behavior note 91) be initialized to TRUE.

**RequireStrongKey** SHOULD[<92>](#Appendix_A_92" \o "Product behavior note 92) be initialized to TRUE.

**domain-name** is a shared Abstract Data Model element with **DomainName.NetBIOS** in ([[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) section 3.2.1.6).

**TrustPasswordVersion** MUST be initialized to 0.

### Higher-Layer Triggered Events

Netlogon responds to a few higher-layer triggered events.

* Transport being added or removed. Whenever a new transport becomes available or unavailable, Netlogon MUST incorporate the transport event and use the DC Locator components ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6) to make sure that it has a valid [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) to connect to.
* If an application calls a Netlogon method and a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is not currently set up, a secure channel MUST be established before the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) call to the server is made.

### Message Processing Events and Sequencing Rules

For all of the method calls, the client MUST bind to the server before making the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) call. If an application calls a Netlogon method and a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is not currently set up, a secure channel MUST be established before the RPC call to the server is made. For details, see sections [3.1.4.6](#Section_f61c3f4a53ff4f3090066d93a2162ef8) and [3.1.4.7](#Section_6b7f7a1c83b7452c9b7b2ece221e236d).

If the *NegotiateFlags* bit L is not set, clients calling the **NetrLogonSamLogon**/**NetrLogonSamLogonEx**/**NetrLogonSamLogonWithFlags** methods MUST have only one outstanding RPC call at a time. If the *NegotiateFlags* bit L is set, clients can have more than one concurrent RPC call.

Whenever a new transport becomes available or unavailable, Netlogon receives a notification, and it uses the DC Locator component ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6) to make sure that it has a valid [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) with which to connect.

#### DC Location Methods

##### Calling DsrGetDcNameEx2

No client-specific events or rules are required.

##### Calling DsrGetDcNameEx

No client-specific events or rules are required.

##### Calling DsrGetDcName

No client-specific events or rules are required.[<93>](#Appendix_A_93" \o "Product behavior note 93)

##### Calling NetrGetDCName

No client-specific events or rules are required.

##### Calling NetrGetAnyDCName

No client-specific events or rules are required.

##### Calling DsrGetSiteName

No client-specific events or rules are required.

##### Calling DsrGetDcSiteCoverageW

No client-specific events or rules are required.

##### Calling DsrAddressToSiteNamesW

No client-specific events or rules are required.

##### Calling DsrAddressToSiteNamesExW

No client-specific events or rules are required.

##### Calling DsrDeregisterDnsHostRecords

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling DsrUpdateReadOnlyServerDnsRecords

The client MUST do the following to call DsrUpdateReadOnlyServerDnsRecords.

* Use the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *ServerName* parameter.[<94>](#Appendix_A_94" \o "Product behavior note 94)
* Pass the client name as the *ComputerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the ReturnAuthenticator, as defined in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).[<95>](#Appendix_A_95" \o "Product behavior note 95)

#### Secure Channel Establishment and Maintenance Methods

##### Calling NetrServerReqChallenge

The client MUST do the following:

* Pass a valid [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) name as the *PrimaryName* parameter.
* Generate 64 bits of random data to pass as the *ClientChallenge* parameter.

##### Calling NetrServerAuthenticate3

To call NetrServerAuthenticate3, the client MUST have called [NetrServerReqChallenge](#Section_5ad9db9f74414ce58c7b7b771e243d32) and have a local copy of the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9).

The client MUST set **ClientStoredCredential** to 0.

The client MUST set **ServerStoredCredential** to 0.

The client MUST compute a Netlogon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) using the algorithm described in section [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585). The result MUST be computed using the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) used in the call to NetrServerReqChallenge. The computed credential is passed as the *ClientCredential* parameter.

If the server returns STATUS\_ACCESS\_DENIED and the client used [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e):

* If RejectMD5Servers is set to FALSE and the *NegotiateFlags* parameter bit flag W is not set, the client SHOULD retry establishing the session with the MD5/DES algorithm.
* If RejectMD5Servers is set to TRUE, the client MUST fail session-key negotiation.

If RequireStrongKey is set to TRUE, and the server did not specify bit O in the *NegotiateFlags* output parameter as described in section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed), the client MUST fail session-key negotiation.

If RequireSignOrSeal is set to TRUE, and the server did not specify bit Y in the *NegotiateFlags* output parameter as described in section 3.1.4.2, the client MUST fail session-key negotiation.

After the call to NetrServerAuthenticate3 completes successfully, the client MUST compute the server Netlogon credential (as specified in section 3.1.4.4) and compare it with the one passed from the server for verification. The result MUST be computed using the server challenge. If the comparison fails, the client MUST fail [**session-key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation.

If the return value indicates that the method is not available on the server, the client MUST retry with a call to [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355). If that call also fails with the method not available on the server, the client MUST retry with a call to [NetrServerAuthenticate](#Section_2561f16011f943a7bad45721a05e8ad8).

The client MUST compute a session key to use for encrypting further communications, as specified in section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63).

The client sets **ConnectionStatus** (section [3.4.5.3.1](#Section_739115d00d16460f96c8775fde606bd5)) if changed.

##### Calling NetrServerAuthenticate2

Message processing is identical to [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9), as specified in section [3.4.5.2.2](#Section_5ce4f403c16e42bc9c6e30d7e319feac), except for the following:

The *AccountRid* parameter is not present in [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355).

##### Calling NetrServerAuthenticate

Message processing is identical to [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9),[<96>](#Appendix_A_96" \o "Product behavior note 96) as specified in section [3.4.5.2.2](#Section_5ce4f403c16e42bc9c6e30d7e319feac), except for the following:

* The *NegotiateFlags* parameter is not present in [NetrServerAuthenticate](#Section_2561f16011f943a7bad45721a05e8ad8).
* The *AccountRid* parameter is not present in NetrServerAuthenticate.

##### Calling NetrServerPasswordSet2

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) that is established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that is identified by domain-name, and pass its name as the *PrimaryName* parameter.
* Encrypt the *ClearNewPassword* parameter using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the **NegotiateFlags** member of the **ServerSessionInfo** table entry for *PrimaryName*) and the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) established as the [**encryption key**](#gt_fbdcfa70-e954-4dbd-bafa-0f9c4bcf90dd).
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

The *ClearNewPassword* parameter is constructed as follows, assuming a WCHAR-represented password of length X bytes.

If the password is for an interdomain account:

* The password is copied into the **Buffer** field of *ClearNewPassword*, which is treated as an array of bytes, starting at byte offset (512 - X).
* An [NL\_PASSWORD\_VERSION](#Section_cba0e87eb91f411b9be86fd321e126b7) structure, as specified in section 2.2.1.3.8, is prepared. The **PasswordVersionNumber** field of the structure is set to the value of the [TrustPasswordVersion](#Section_708b71329e72447c992bd0bef4078f81) variable corresponding to the password being set. The first [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password generated has **TrustPasswordVersion** equal to one. Each time a new trust password is generated, its **TrustPasswordVersion** is computed by adding one to the value of **TrustPasswordVersion** of the previous password. The NL\_PASSWORD\_VERSION structure is copied into ClearNewPassword.Buffer starting at byte offset (512 - X - size of (NL\_PASSWORD\_VERSION)). For more information on the NL\_PASSWORD\_VERSION structure, see section 2.2.1.3.8.
* The first (512 - X) - size of (NL\_PASSWORD\_VERSION) bytes of ClearNewPassword.Buffer are filled with randomly generated data.
* ClearNewPassword.Length is set to X.

For any other type of account:

* The password is copied into the **Buffer** field of *ClearNewPassword*, which is treated as an array of bytes, starting at byte offset (512 - X).
* The first (512 - X) bytes are filled with randomly generated data.
* ClearNewPassword.Length is set to X.

After the method returns, the client MUST verify the ReturnAuthenticator as defined in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<97>](#Appendix_A_97" \o "Product behavior note 97) re-establish the secure channel with the domain controller.

##### Calling NetrServerPasswordSet

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *PrimaryName* parameter.
* Pass the encrypted new password:
  1. Compute the NTOWFv1 ([[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the new password.
  2. Encrypt ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.11.1.1) the result of step 1 using the Session-Key for the secure channel as the specified key.
  3. Pass the result of step 2 as the *UasNewPassword* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the ReturnAuthenticator as described in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<98>](#Appendix_A_98" \o "Product behavior note 98) re-establish the secure channel with the domain controller.

##### Calling NetrServerPasswordGet

The client calling this method MUST be a BDC. The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name and pass its name as the *ServerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

The client MUST decrypt the *EncryptedNtOwfPassword* return parameter that was encrypted (as described in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.11.1.1) with the Session-Key for the secure channel as the specified key.

After the method returns, the client MUST verify the *ReturnAuthenticator* as defined in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<99>](#Appendix_A_99" \o "Product behavior note 99) reestablish the secure channel with the domain controller.

##### Calling NetrServerTrustPasswordsGet

The process for calling NetrServerTrustPasswordsGet is the same as that used for [NetrServerGetTrustInfo](#Section_4c2296c3c6f047fc9f01a6fe17bf1d5b), except the *TrustInfo* parameter is not specified.

See section [3.4.5.5.6](#Section_6482836222d940d48cc2bfad92f50964), Calling NetrServerGetTrustInfo.

##### Calling NetrLogonGetDomainInfo

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *ServerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.
* Pass the *Level* parameter set to 1 or 2.

After the method returns, the client MUST verify the *ReturnAuthenticator* as defined in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<100>](#Appendix_A_100" \o "Product behavior note 100) re-establish the secure channel with the domain controller.

##### Calling NetrLogonGetCapabilities

The client SHOULD[<101>](#Appendix_A_101" \o "Product behavior note 101) do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *ServerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the *ReturnAuthenticator* (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)) and compare the received **Capabilities** with the negotiated flags of the current secure channel. If the negotiated flags do not match, then the client SHOULD[<102>](#Appendix_A_102" \o "Product behavior note 102) re-establish the secure channel with the DC.

Upon receiving STATUS\_NOT\_IMPLEMENTED, the client MUST treat this as successful confirmation that the DC does not support [**AES**](#gt_21edac94-99d0-44cb-bc1a-3416d8fc618e) [[FIPS197]](https://go.microsoft.com/fwlink/?LinkId=89870).[<103>](#Appendix_A_103" \o "Product behavior note 103)

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<104>](#Appendix_A_104" \o "Product behavior note 104) re-establish the secure channel with the DC.

##### Calling NetrChainSetClientAttributes

The [**read-only domain controller**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a normal (writable) [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name and pass its name as the *ServerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.
* Pass the *dwInVersion* parameter set to 1.
* Pass the address of a valid [NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1](#Section_ab43a76224e245c387011838589d80fe) structure as the *pmsgIn* parameter.
* Pass the *pdwOutVersion* parameter set to the address of the value 1.
* Pass the address of a valid NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 structure as the *pmsgOut* parameter.

After the method returns, the client MUST verify the ReturnAuthenticator, as specified in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD reestablish the secure channel with the normal (writable) DC.[<105>](#Appendix_A_105" \o "Product behavior note 105)

#### Pass-Through Authentication Methods

All clients SHOULD set **ConnectionStatus** (section [3.4.5.3.1](#Section_739115d00d16460f96c8775fde606bd5)) if changed.

##### Setting ConnectionStatus

When one of the following return values is received, the client SHOULD set **ConnectionStatus** to that value:

* NERR\_Success
* STATUS\_NO\_LOGON\_SERVERS
* STATUS\_ACCESS\_DENIED
* STATUS\_NO\_TRUST\_LSA\_SECRET
* STATUS\_NO\_TRUST\_SAM\_ACCOUNT
* STATUS\_INVALID\_SERVER\_STATE
* STATUS\_NO\_MEMORY
* STATUS\_INSUFFICIENT\_RESOURCES
* STATUS\_DISK\_FULL

##### Calling NetrLogonSamLogonEx

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name and pass its name as the *LogonServer* parameter.
* Pass the client name as the *ComputerName* parameter.
* If the *LogonLevel* is [NetlogonInteractiveInformation](#Section_8c7808e54e5c420e9c9047286da2218f) or NetlogonInteractiveTransitiveInformation, the client SHOULD[<106>](#Appendix_A_106" \o "Product behavior note 106) encrypt the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_INTERACTIVE\_INFO](#Section_af76351fef6946bca451e4c4b99bac4a) structure.
* If the *LogonLevel* is NetlogonServiceInformation or NetlogonServiceTransitiveInformation, encrypt[<107>](#Appendix_A_107" \o "Product behavior note 107) the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_SERVICE\_INFO](#Section_1c9f2af2e16445489428eae68a03537e) structure.
* If the *LogonLevel* is NetlogonGenericInformation, then encrypt[<108>](#Appendix_A_108" \o "Product behavior note 108) the **LogonData** member in the [NETLOGON\_GENERIC\_INFO](#Section_c03d6d959b5e43299645eedcdd167f6e) structure.
* Call the method using Secure [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331), as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.1.5.2.1.

If the *NegotiateFlags* bit V is not set, then the [**read-only domain controller (RODC)**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) SHOULD NOT set *ExtraFlags* C or D.

If the *NegotiateFlags* bit P is set, then the client SHOULD convert:

* NetlogonInteractiveInformation to NetlogonInteractiveTransitiveInformation
* NetlogonNetworkInformation to NetlogonNetworkTransitiveInformation
* NetlogonServiceInformation to NetlogonServiceTransitiveInformation

If the *NegotiateFlags* bit G is not set and *LogonLevel* is not NetlogonGenericInformation, then the *ValidationLevel* parameter MUST be set to 2 ([NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11)](#Section_142a277fe16145ac8b95b94bb169b5da)).

The *LogonLevel*, *LogonInformation*, *ValidationLevel*, and *ValidationInformation* parameters are specified in [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) for NTLM, Kerberos, and Digest, and in [[MS-RCMP]](%5bMS-RCMP%5d.pdf#Section_5462719690dd4e968c7f7520066785ba) for TLS/SSL.

To call for Generic-Passthrough to authentication packages, the *LogonLevel* parameter MUST be set to 4 (NetlogonGenericInformation), and the *ValidationLevel* parameter MUST be set to 5 ([NetlogonValidationGenericInfo2](#Section_95154ae4d30543e582e4d5353e0f117c)). The *LogonInformation* parameter MUST be a NETLOGON\_GENERIC\_INFO structure, as specified in section 2.2.1.4.2.

After the method returns, the client MUST:

* If the *LogonLevel* is **NetlogonNetworkInformation** or **NetlogonNetworkTransitiveInformation**, the client MUST decrypt the *UserSessionKey* and the first two elements of the **ExpansionRoom** array in the NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11) or in the [NETLOGON\_VALIDATION\_SAM\_INFO2 (section 2.2.1.4.12)](#Section_2a12e28979044ecb9d836732200230c0) structure.
* Verify that it received an [**authoritative response**](#gt_1ed0d067-3bfd-4fd5-a68a-5e947d379858) by checking the *Authoritative* parameter. If the *Authoritative* parameter is TRUE, the client MUST treat the result as final. If the *Authoritative* parameter is FALSE, the client SHOULD retry the call at a later time or at a different domain controller.

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD re-establish the secure channel with the DC. [<109>](#Appendix_A_109" \o "Product behavior note 109)

##### Calling NetrLogonSamLogonWithFlags

Message processing for NetrLogonSamLogonWithFlags is identical to [NetrLogonSamLogon](#Section_20cf9342c1fa49ada9a96d5f52e444fd), except for the following:

* NetrLogonSamLogonWithFlags has the additional parameter *ExtraFlags*.

See section 3.4.5.3.4.

##### Calling NetrLogonSamLogon

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *LogonServer* parameter.
* Pass the client name as the *ComputerName* parameter.
* If the *LogonLevel* is [NetlogonInteractiveInformation](#Section_8c7808e54e5c420e9c9047286da2218f) or NetlogonInteractiveTransitiveInformation, then encrypt[<110>](#Appendix_A_110" \o "Product behavior note 110) the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_INTERACTIVE\_INFO](#Section_af76351fef6946bca451e4c4b99bac4a) structure.
* If the *LogonLevel* is NetlogonServiceInformation or NetlogonServiceTransitiveInformation, then encrypt[<111>](#Appendix_A_111" \o "Product behavior note 111) the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_SERVICE\_INFO](#Section_1c9f2af2e16445489428eae68a03537e) structure.
* If the *LogonLevel* is NetlogonGenericInformation, then encrypt[<112>](#Appendix_A_112" \o "Product behavior note 112) the **LogonData** member in the [NETLOGON\_GENERIC\_INFO](#Section_c03d6d959b5e43299645eedcdd167f6e) structure.
* If the *LogonLevel* is **NetlogonNetworkInformation** or **NetlogonNetworkTransitiveInformation**, then encrypt the *UserSessionKey* and the first two elements of the **ExpansionRoom** array in the [NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11)](#Section_142a277fe16145ac8b95b94bb169b5da) or in the [NETLOGON\_VALIDATION\_SAM\_INFO2 (section 2.2.1.4.12)](#Section_2a12e28979044ecb9d836732200230c0) structure.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

If the *NegotiateFlags* bit P is set, then the client SHOULD convert:

* NetlogonInteractiveInformation to NetlogonInteractiveTransitiveInformation
* NetlogonNetworkInformation to NetlogonNetworkTransitiveInformation
* NetlogonServiceInformation to NetlogonServiceTransitiveInformation

If the *NegotiateFlags* bit G is not set and *LogonLevel* is not NetlogonGenericInformation, then the *ValidationLevel* parameter MUST be set to 2 (NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11)).

The *LogonLevel*, *LogonInformation*, *ValidationLevel*, and *ValidationInformation* parameters are specified in [[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) for NTLM, Kerberos, and Digest, and in [[MS-RCMP]](%5bMS-RCMP%5d.pdf#Section_5462719690dd4e968c7f7520066785ba) for TLS/SSL.

To call for Generic-Passthrough to authentication packages, the *LogonLevel* parameter MUST be set to 4 (NetlogonGenericInformation), and the *ValidationLevel* parameter MUST be set to 5 ([NetlogonValidationGenericInfo2](#Section_95154ae4d30543e582e4d5353e0f117c)). The *LogonInformation* parameter MUST be a NETLOGON\_GENERIC\_INFO structure, as specified in section 2.2.1.4.2.

After the method returns, the client MUST:

* Verify the *ReturnAuthenticator*, as specified in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).
* Verify that it received an [**authoritative response**](#gt_1ed0d067-3bfd-4fd5-a68a-5e947d379858) by checking the *Authoritative* parameter. If the *Authoritative* parameter is TRUE, the client MUST treat the result as final. If the *Authoritative* parameter is FALSE, the client SHOULD retry the call at a later time or at a different domain controller.

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD reestablish the secure channel with the DC.[<113>](#Appendix_A_113" \o "Product behavior note 113)

##### Calling NetrLogonSamLogoff

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *LogonServer* parameter.
* Pass the client name as the *ComputerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the *ReturnAuthenticator* as described in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD reestablish the secure channel with the DC.[<114>](#Appendix_A_114" \o "Product behavior note 114)

#### Account Database Replication Methods

##### Calling NetrDatabaseDeltas

The client calling this method MUST be a BDC. It MUST do the following:

* Pass a valid [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) name as the *PrimaryName* parameter.
* Pass the client BDC name as the *ComputerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.
* Pass a valid [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) identifier as the *DatabaseID* parameter as follows:
  + For the [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b), the *DatabaseID* parameter MUST be 0x00000000.
  + For the SAM built-in database, the *DatabaseID* parameter MUST be 0x00000001.
  + For the [**LSA database**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b), the *DatabaseID* parameter MUST be 0x00000002.
* Pass the value of the local [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) as the *DomainModifiedCount*.
* Pass the preferred maximum length of data to be returned in the DeltaArray parameter as the *PreferredMaximumLength* parameter.

On receiving the STATUS\_MORE\_ENTRIES status code, the client continues calling this routine in a loop updating DomainModifiedCount until all missing database entries are received. On receiving the STATUS\_SUCCESS status code, the client terminates the loop. The client MAY terminate the loop early without receiving all entries. For example, the client MAY choose to do so on a system shutdown notification.

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD [<115>](#Appendix_A_115" \o "Product behavior note 115) reestablish the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

##### Calling NetrDatabaseSync2

The client calling this method MUST be a BDC. The client SHOULD[<116>](#Appendix_A_116" \o "Product behavior note 116) call this method in a loop (referred to in this section as the synchronization loop) until all [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) records are received as indicated by the return code STATUS\_SUCCESS.

The client MUST do the following:

* Pass a valid [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) name as the *PrimaryName* parameter.
* Pass the client BDC name as the *ComputerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.
* Pass a valid database identifier as the *DatabaseID* parameter as follows:
  + For the [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b), the *DatabaseID* parameter MUST be 0x00000000.
  + For the SAM built-in database, the *DatabaseID* parameter MUST be 0x00000001.
  + For the [**LSA database**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b), *DatabaseID* MUST be 0x00000002.
* Set *RestartState* to NormalState unless this call is a restart of a synchronization loop, in which case set *RestartState* as follows:
  + GroupState if the last [**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e) type of the previous synchronization loop was AddOrChangeGroup.
  + UserState if the last delta type of the previous synchronization loop was AddOrChangeUser.
  + GroupMemberState if the last delta type of the previous synchronization loop was ChangeGroupMembership.
  + AliasState if the last delta type of the previous synchronization loop was AddOrChangeAlias.
  + AliasMemberState if the last delta type of the previous synchronization loop was ChangeAliasMembership.
* If this is a first call in a synchronization loop, pass *SyncContext* as 0x00000000. Otherwise, pass *SyncContext* as the *SyncContext* value returned by the previous call in a synchronization loop, either continued as normal or terminated.
* Pass the preferred maximum length of data to be referenced in the *DeltaArray* parameter as the *PreferredMaximumLength* parameter.

On receiving the STATUS\_MORE\_ENTRIES status code, the client SHOULD[<117>](#Appendix_A_117" \o "Product behavior note 117) continue calling this routine in a loop until all missing database entries are received. On receiving the STATUS\_SUCCESS status code, the client MUST terminate the loop. The client MAY terminate the loop early on without receiving all entries. For example, the client MAY choose to do so on a system shutdown notification. In that case, if the client intends to restart the synchronization loop at a later point, the client MUST maintain the state for setting the *RestartState* parameter to restart the loop as previously described.

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<118>](#Appendix_A_118" \o "Product behavior note 118) re-establish the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

##### Calling NetrDatabaseSync

Calling this method is identical to calling [NetrDatabaseSync2](#Section_b9acd7feee244bb0a3ff085c4b98284d), as specified in section 3.4.5.4.2, except that this call does not use the *RestartState* parameter, as it doesn't support restarting the synchronization loop.

##### Calling NetrDatabaseRedo

The client calling this method MUST be a BDC. The client MUST do the following:

* Pass a valid [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) name as the *PrimaryName* parameter.
* Pass the client BDC name as the *ComputerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.
* Pass a valid single account object information request message as described in the CHANGELOG\_ENTRY structure in section [3.5.4.6.4](#Section_c8352ce88b094baeaaf7456d7e6fda6c).
* Pass the size of the single account object information request message as the *ChangeLogEntrySize* parameter.

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<119>](#Appendix_A_119" \o "Product behavior note 119) reestablish the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

#### Domain Trusts Methods

##### Calling DsrEnumerateDomainTrusts

No client-specific events or rules are required.

##### Calling NetrEnumerateTrustedDomainsEx

No client-specific events or rules are required.

##### Calling NetrEnumerateTrustedDomains

No client-specific events or rules are required.

##### Calling NetrGetForestTrustInformation

The client calling this method MUST be a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in a different [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). If the NegotiateFlags bit T is not set, then the client SHOULD NOT call this method.

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a domain controller in the domain identified by domain-name and pass its name as the *ServerName* parameter.
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the *ReturnAuthenticator* as described in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<120>](#Appendix_A_120" \o "Product behavior note 120) reestablish the secure channel with the domain controller.

##### Calling DsrGetForestTrustInformation

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrServerGetTrustInfo

The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name, and pass its name as the *TrustedDcName* parameter.

After the method returns, the client MUST verify the *ReturnAuthenticator* as described in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).

On receiving STATUS\_ACCESS\_DENIED, the client SHOULD[<121>](#Appendix_A_121" \o "Product behavior note 121) reestablish the secure channel with the domain controller.

#### Message Protection Methods

##### Calling NetrLogonGetTrustRid

If the client requires the [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) for the computer account of the calling machine, the caller MUST specify this by passing NULL for both the *ServerName* and *DomainName* parameters. Otherwise, a valid *ServerName* MUST be passed. The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrLogonComputeServerDigest

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrLogonComputeClientDigest

When comparing digests, the client SHOULD compare the new password digest first. If this comparison fails, the client SHOULD compare the old password digest. If that comparison also fails, the digests do not match. The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrLogonSendToSam

The client calling this method MUST be a BDC or [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870). The client MUST do the following:

* Have a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) established with a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) identified by domain-name and pass its name as the *PrimaryName* parameter.
* Encrypt the *OpaqueBuffer* parameter using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the **NegotiateFlags** member of the **ServerSessionInfo** table entry for *PrimaryName*) and the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) established as the [**encryption key**](#gt_fbdcfa70-e954-4dbd-bafa-0f9c4bcf90dd).
* Pass a valid client Netlogon [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) as the *Authenticator* parameter.

After the method returns, the client MUST verify the *ReturnAuthenticator* as described in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806).[<122>](#Appendix_A_122" \o "Product behavior note 122)

For details about how the *OpaqueBuffer* parameter is used, see [[MS-SAMS]](%5bMS-SAMS%5d.pdf#Section_2e785e4ed5b64ae3b479351a50830921).

##### Calling NetrLogonSetServiceBits

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrLogonGetTimeServiceParentDomain

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

#### Administrative Services Methods

##### Calling NetrLogonControl2Ex

The client MUST do the following:

Supply the *Data* parameter if the client is calling with one of the following *FunctionCode* values:

* 0x00000005(NETLOGON\_CONTROL\_REDISCOVER)
* 0x00000006(NETLOGON\_CONTROL\_TC\_QUERY)
* 0x00000008(NETLOGON\_CONTROL\_FIND\_USER)
* 0x00000009(NETLOGON\_CONTROL\_CHANGE\_PASSWORD)
* 0x0000000A(NETLOGON\_CONTROL\_TC\_VERIFY)

For details about the *FunctionCode* values, see section [3.5.4.9.1](#Section_df7e5dd1ebcc47549da02e0bded82d29).

The client SHOULD be prepared to handle ERROR\_ACCESS\_DENIED, if the server determines that the client does not have appropriate [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940).

##### Calling NetrLogonControl2

The client MUST not use this method for calls requiring *QueryLevel* set to 4. All other client requirements are identical to NetrLogonControl2Ex (section [3.4.5.7.1](#Section_5c506b48dd6b40209a504f93b9f8c7c1)).

##### Calling NetrLogonControl

No client-specific events or rules are required.

#### Obsolete Methods

##### Calling NetrLogonUasLogon

This method was used only by LAN Manager clients and is not currently used.

##### Calling NetrLogonUasLogoff

This method was used only by LAN Manager clients and is not currently used.

##### Calling NetrAccountDeltas

This method supports LAN Manager products.

##### Calling NetrAccountSync

This method supports LAN Manager products.

### Timer Events

#### Timer Expiry on domainControllerCacheTimer

This event occurs whenever the domainControllerCacheTimer expires.

If the client is a [**domain controller (DC)**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the client MUST get a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) list by performing the external behavior consistent with locally invoking LsarEnumerateTrustedDomains ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.8).

* The *EnumerationContext* parameter MUST be set to 0.
* The *PreferredMaximumLength* SHOULD[<123>](#Appendix_A_123" \o "Product behavior note 123) be set to 4096.
* A policy handle is not needed locally.

The client MUST attempt to locate a DC (section [3.1.4.10](#Section_00ac739d274d434b9efbfad10405721a)) for each of the domain entries of the returned trusted domain list.

* If the client fails when attempting to locate a DC for a domain entry in the trusted domain list, the client MUST ignore errors and continue to attempt to locate DCs for the remaining domain entries in the trusted domain list.
* For each successfully located DC: If the DomainControllerInfo.Flags has bit G set, and the ServerSessionInfo table's entry **PrimaryName** field whose **DomainName** field matches the **DomainControllerInfoW.DomainName** field does not match the **DomainControllerInfoW.DomainControllerName** field, the client MUST update the name in **PrimaryName** so that it matches **DomainControllerInfoW.DomainControllerName**. The client also MUST attempt to establish a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) with the located DC (section 3.1.4.10).

### Other Local Events

No additional local events are used on the client beyond the events maintained in the underlying [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a) and GP notification.

When Netlogon receives a PolicyChange event ([[MS-GPOD]](%5bMS-GPOD%5d.pdf#Section_6e6349392ccf4412b75f0035dc05ea67) section 2.8.2), NRPC implementations that persistently store and retrieve the **RequireStrongKey** and **RequireSignOrSeal** variables as defined in section [3.4.1](#Section_fd1e918135a045d3b39cb7453dfc0af5) SHOULD[<124>](#Appendix_A_124" \o "Product behavior note 124) load the new value.

## Netlogon Server Details

### Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

A Netlogon Remote Protocol server maintains the following abstract variables, in addition to the ones defined in section [3.1](#Section_273b6905782d4a7ea2e44337816916e0):

**NetlogonSecurityDescriptor:** A security descriptor that is used for verifying access security during processing of some methods. This security descriptor MUST NOT be changed.

**ServerCapabilities:** A 32-bit set of bit flag options defined in section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed) that identify the server's supported options.

**DNSDomainName:** The [**FQDN (2)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) for the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) to which the server belongs. This ADM element is shared with **DomainName.FQDN** ([[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) section 3.2.1.6).

**NetbiosDomainName:** The NetBIOS domain name for the domain to which the server belongs. This ADM element is shared with **DomainName.NetBIOS** [MS-WKST] section 3.2.1.6).

**DomainGuid:** The [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) for the domain. This ADM element is shared with **DomainGuid** ([MS-WKST] section 3.2.1.6).

**DomainSid:** The [**security identifier**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) for the domain. This ADM element is shared with **DomainSid** ([MS-WKST] section 3.2.1.6).

**AllowSingleLabelDNSDomain:** A Boolean that specifies whether [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) location via single label [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) names is enabled.

**AllowDnsSuffixSearch:** A Boolean that specifies whether DC location via single-label domains using DNS suffix composition is enabled.

**SiteName:** The [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) name of the computer.

**NextClostestSiteName:** The name of the site that is closest to the site of the computer.

**DynamicSiteName:** Dynamically determined site name of the computer.

**DynamicSiteNameTimeout:** An implementation-specific time span that determines whether it SHOULD[<125>](#Appendix_A_125" \o "Product behavior note 125) be time to rediscover the site name.

**DynamicSiteNameSetTime:** An implementation-specific timestamp indicating the time at which DynamicSiteName was determined.

**ChallengeTable:** A table indexed by **ComputerName** with the following members:

* **ComputerName:** The **ComputerName** (section [3.5.4.4.1](#Section_5ad9db9f74414ce58c7b7b771e243d32)) used by the DC during [session-key negotiations (section 3.1.4.1)](#Section_7b9e31d1670e4fc5ad549ffff50755f9).
* **ClientChallenge:** A pointer to a [NETLOGON\_CREDENTIAL (section 2.2.1.3.4)](#Section_d55e263271634f6cb6624b870e8cc1cd) structure that contains the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473).
* **ServerChallenge:** A pointer to a NETLOGON\_CREDENTIAL structure that contains the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9) response.
* **SecureChannelType:** A [NETLOGON\_SECURE\_CHANNEL\_TYPE (section 2.2.1.3.13)](#Section_4d1235e32c964e9fa1473cb338a0d09f) enumerated value, as specified in section 2.2.1.3.13, that indicates the type of the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) being established.

**FailedDiscoveryCache:** The server SHOULD implement a cache containing a set of failed DC discovery attempts. The fields of the cache are implementation-specific but any cache implementation MUST be able to return the time when the last DC discovery attempt failed for a given domain name (see section [3.5.4.3.1](#Section_fb8e1146a0454c3198d1c68507ad5620) for more information).

**FailedDiscoveryCachePeriod:** The length of time, in seconds, for which an entry in the **FailedDiscoveryCache** is valid.

**CacheEntryValidityPeriod:** The length of time, in hours, for which an entry in the **LocatedDCsCache** is valid.

**CacheEntryPingValidityPeriod:** The length of time, in minutes, for which an entry in the **LocatedDCsCache** is considered valid without having to ping the DC represented by that cached entry.

The Netlogon server variables which are registry keys are as follows:

**RejectMD5Clients:** A Boolean variable that indicates whether the server SHOULD[<126>](#Appendix_A_126" \o "Product behavior note 126) reject incoming clients that are using MD5 encryption.

**SignSecureChannel:** A Boolean variable that determines whether a [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) attempts to negotiate signing for all secure channel traffic that it initiates.

**TrustedDomains:** A list of domain [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) (of type [DS\_DOMAIN\_TRUSTSW (section 2.2.1.6.2)](#Section_7de9866ed3ef4a9f98a5c2dcff1e61c1)) obtained by calling [DsrEnumerateDomainTrusts (section 3.5.4.7.1)](#Section_f98236242b34415cbdca9f9a6d97016b).

When the server is a DC, it also maintains the following abstract variables:

**RejectDES:** A Boolean variable that indicates whether the server MUST reject incoming clients using DES encryption in ECB mode.

**DnsForestName:** The FQDN (2) [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) name for the forest to which the domain belongs. The **DnsForestName** value is configured as described in [MS-WKST] and is shared with **DomainName.FQDN** ([MS-WKST] section 3.2.1.6).

**LogonAttempts:** A 32-bit unsigned integer shared from LogonAttempts ([[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 3.1.1).

**NT4Emulator:** A Boolean variable that indicates whether the server offers only the server capabilities of a Windows NT 4.0 unless the client specifically requests otherwise.[<127>](#Appendix_A_127" \o "Product behavior note 127)

**RefusePasswordChange:** A setting that indicates whether the server refuses client password changes. This domain-wide setting can be used to indicate to the client machines that they SHOULD avoid password changes. When TRUE, the *NegotiateFlags* bit I is sent.

**DCRPCPort:** The domain controller Netlogon port that SHOULD[<128>](#Appendix_A_128" \o "Product behavior note 128) be registered with the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee) mapper instead of the standard dynamic port. It is read only once, at initialization.

**SiteCoverage:** The names of all the sites that a domain controller covers.

**TrustedDomainObjectsCollection:** A collection of trusted domain objects as defined and initialized in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.1.5.

The server also maintains the following abstract variable for BDC replication:

**SynchronizationComplete:** A Boolean variable that indicates that [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) synchronization is complete.

When a secure channel is established, the server maintains:

**ClientSessionInfo**: A table indexed by *ComputerName* with the following members:

* **ComputerName**: The *ComputerName* (section 3.5.4.4.1) used by the DC during session-key negotiations (section 3.1.4.1).
* **ClientSequenceNumber**: See section [3.3.1](#Section_a7bd20030d614686aa6e89336cec83a1) for *ClientSequenceNumber* details.
* **AccountRid**: The [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of this client's machine account.
* **ServerSequenceNumber**: See section 3.3.1 for *ServerSequenceNumber* details.
* **Session-Key**: See section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63) for *Session-Key* computation details.
* **NegotiateFlags**: See section [3.1.1](#Section_708b71329e72447c992bd0bef4078f81) for *NegotiateFlags* details.
* **ServerStoredCredential**: See section 3.1.1 for *ServerStoredCredential* details.
* **SecureChannelType**: A **NETLOGON\_SECURE\_CHANNEL\_TYPE** enumerated value, as specified in section 2.2.1.3.13, which indicates the type of secure channel being established with this client.

In addition, NetLogon stores service state information.

**ServerServiceBits:** A set of bit flags used to store the state of running services. If the bit is set to 0, the corresponding service is not running; otherwise, the bit is set to 1 and the corresponding service is running. The value of the bit flags is constructed from zero or more bit flags in the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | 0 | 0 | 0 | B | 0 | 0 | A | 0 | 0 | 0 | 0 | 0 | 0 |

The meanings of the flags are described in the following table.

| Value | Description |
| --- | --- |
| A | The time service is running. |
| B | The time service with clock hardware is running. |
| C | The Active Directory Web service is running. |

### Timers

None.

### Initialization

The server side registers an [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee) with [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) over named pipes transport, using the NETLOGON named pipe[<129>](#Appendix_A_129" \o "Product behavior note 129) and an endpoint with RPC over TCP/IP. When DCRPCPort is present and is not NULL, and the [**server**](#gt_434b0234-e970-4e8c-bdfa-e16a30d96703) is a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), then the DC MUST also register the port listed in DCRPCPort ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.3.3.1.4). The server side MUST register the Netlogon [**security support provider (SSP)**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a) authentication\_type constant [0x44] as the [**security provider**](#gt_05fd3925-0672-4f24-9dd9-2b9d441eb333) ([MS-RPCE] section 3.3.3.3.1.3) used by the RPC interface.

**NetlogonSecurityDescriptor**: Initialized to the following value, expressed in Security Descriptor Description Language (SDDL) ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.5.1): D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU) S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)

**ChallengeTable** MUST be empty.

**ClientSessionInfo** MUST be empty.

**RefusePasswordChange** SHOULD be FALSE.

The **ServerCapabilities** field SHOULD be initialized to reflect the capabilities offered by that server implementation.

**RejectMD5Clients** SHOULD[<130>](#Appendix_A_130" \o "Product behavior note 130) be initialized in an implementation-specific way and SHOULD be FALSE.

**SealSecureChannel** SHOULD be TRUE.

**SignSecureChannel** SHOULD[<131>](#Appendix_A_131" \o "Product behavior note 131) be initialized in an implementation-specific way and SHOULD be TRUE. Any changes made to the **SignSecureChannel** registry keys are reflected in the ADM elements when a PolicyChange event is received (section [3.1.6](#Section_6e9975e7c21d4ec5aafc0dfdf7325ebe)).

**StrongKeySupport** SHOULD[<132>](#Appendix_A_132" \o "Product behavior note 132) be TRUE.

**NetbiosDomainName** is a shared ADM element with **DomainName.NetBIOS** ([[MS-WKST]](%5bMS-WKST%5d.pdf#Section_5bb08058bc364d3cabebb132228281b7) section 3.2.1.6).

**DomainGuid**: Prior to the initialization of the Netlogon Remote Protocol, **DomainGuid** has already been initialized, as described in [MS-WKST] section 3.2.1.6, since Netlogon Remote Protocol is running on a system already joined to a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**DomainSid**: Prior to the initialization of the Netlogon Remote Protocol, **DomainSid** has already been initialized, as described in [MS-WKST] section 3.2.1.6, since Netlogon Remote Protocol is running on a system already joined to a domain.

**AllowSingleLabelDNSDomain** SHOULD[<133>](#Appendix_A_133" \o "Product behavior note 133) be set to a locally configured value.

**AllowDnsSuffixSearch** SHOULD[<134>](#Appendix_A_134" \o "Product behavior note 134) be set to TRUE.

**SiteName** SHOULD[<135>](#Appendix_A_135" \o "Product behavior note 135) be initialized from msDS-SiteName ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.4.5.29) of the [**computer object**](#gt_d8e8f5a7-db85-40a8-98ed-1abab2237b82) if the server is a DC. If the server is not a DC, this ADM element is set to a locally configured value.

**NextClosestSiteName** SHOULD be initialized as follows: if the server is a DC, the server SHOULD invoke IDL\_DRSQuerySitesByCost ([[MS-DRSR]](%5bMS-DRSR%5d.pdf#Section_f977faaa673e4f66b9bf48c640241d47) section 4.1.16), setting **NextClosestSiteName** to the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) that is closest to **SiteName** but not equal to **SiteName**. If the server is not a DC, this ADM element SHOULD be initialized to NULL.

**DynamicSiteNameSetTime** MUST be set to a value such that **DynamicSiteNameSetTime** plus **DynamicSiteNameTimeout** is less than the current time.

**FailedDiscoveryCachePeriod** SHOULD[<136>](#Appendix_A_136" \o "Product behavior note 136) be set to a locally configured value.

**CacheEntryValidityPeriod** SHOULD[<137>](#Appendix_A_137" \o "Product behavior note 137) be set to a locally configured value.

**CacheEntryPingValidityPeriod** SHOULD[<138>](#Appendix_A_138" \o "Product behavior note 138) be set to a locally configured value.

If the NRPC server is a DC, then the following abstract data model variables are initialized:

* **DCRPCPort** SHOULD[<139>](#Appendix_A_139" \o "Product behavior note 139) be initialized in an implementation-specific way and MUST default to NULL.
* **DnsForestName**: SHOULD be initialized from the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) of **rootDomainNamingContext** ([MS-ADTS] section 3.1.1.3.2.16).
* The objects in **TrustedDomainObjectsCollection** are initialized as described in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.1.5.
* The **NT4Emulator** field SHOULD be FALSE.
* **RejectDES** SHOULD[<140>](#Appendix_A_140" \o "Product behavior note 140) be initialized in an implementation-specific way and SHOULD[<141>](#Appendix_A_141" \o "Product behavior note 141) default to TRUE. .
* **ServerServiceBits** SHOULD be initialized to zero.
* **SiteCoverage** SHOULD be initialized in an implementation-specific way and MUST default to NULL. Implementations SHOULD[<142>](#Appendix_A_142" \o "Product behavior note 142) persistently store and retrieve the **SiteCoverage** variable.

### Message Processing Events and Sequencing Rules

The following section specifies data and state maintained by the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) server. It includes details about receiving Netlogon RPC methods on the server side of the client/server communication. The provided data is to facilitate the explanation of how the protocol behaves. This section does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

This protocol MUST instruct the RPC runtime, via the **strict\_context\_handle** attribute, to reject use of context handles created by a method of a different RPC interface than this one, as described in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.

This protocol MUST indicate to the RPC runtime that it is to perform a strict NDR data consistency check at target level 6.0, as specified in [MS-RPCE] section 3.

Methods in RPC Opnum Order

| Method | Description |
| --- | --- |
| [NetrLogonUasLogon](#Section_4db6051c9876446c957dc8f6aecbdb9a) | This method was for support of LAN Manager products, and it is no longer used. This method was introduced in LAN Manager.  Opnum: 0 |
| [NetrLogonUasLogoff](#Section_f89840bc42154dc89d365c1e5fa6a77d) | This method was for support of LAN Manager products, and it is no longer used. This method was introduced in LAN Manager.  Opnum: 1 |
| [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a) | The NetrLogonSamLogon method updates the user's **lastLogon** attribute for the [**Security Account Manager (SAM)**](#gt_0b53d5bb-74ab-4705-8657-c22d32781103).  Opnum: 2 |
| [NetrLogonSamLogoff](#Section_a087dc875d4b40228f9156ac2dc20256) | The NetrLogonSamLogoff method handles logoff requests for the SAM.  Opnum: 3 |
| [NetrServerReqChallenge](#Section_5ad9db9f74414ce58c7b7b771e243d32) | The NetrServerReqChallenge method receives a [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) and returns a server challenge.  Opnum: 4 |
| [NetrServerAuthenticate](#Section_2561f16011f943a7bad45721a05e8ad8) | The NetrServerAuthenticate method authenticates an account by verifying that the computed client [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) are the same as those provided in the previous challenge.  Opnum: 5 |
| [NetrServerPasswordSet](#Section_a93310347f3047bd8aee93bbabe90df4) | The NetrServerPasswordSet method sets a new password for an account in the User Account Subsystem (UAS).  Opnum: 6 |
| [NetrDatabaseDeltas](#Section_5412f0bc5eb94197b4c4c5a8c06ba018) | The NetrDatabaseDeltas method returns a set of recent actions performed on the [**Security Account Manager (SAM) database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b), along with the number of times the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) has been modified.  Opnum: 7 |
| [NetrDatabaseSync](#Section_86683ada19a2414eafaf124f77dc4685) | The NetrDatabaseSync method provides an interface to synchronize a [**backup domain controller's**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3) Security Account Manager (SAM) database to that of the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) by means of replication.  Opnum: 8 |
| [NetrAccountDeltas](#Section_9a4ba74c00474053bd51d6204f291710) | The NetrAccountDeltas method supported LAN Manager BDCs, and is no longer supported.  Opnum: 9 |
| [NetrAccountSync](#Section_717064350c2b4fd999abb27f28dc9ae0) | The NetrAccountSync method supported LAN Manager BDCs, and is no longer supported.  Opnum: 10 |
| [NetrGetDCName](#Section_ddd7452f4b7d47e6895b5b23d9dd2120) | The NetrGetDCName method retrieves the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the PDC for a specified domain.  Opnum: 11 |
| [NetrLogonControl](#Section_d62ebadc996749efa48db4059a7176c5) | The NetrLogonControl method executes a specific Netlogon control operation.  Opnum: 12 |
| [NetrGetAnyDCName](#Section_3db726ac0d1b43bebd6f923d97768436) | The NetrGetAnyDCName method retrieves the name of a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in a specified domain.  Opnum: 13 |
| [NetrLogonControl2](#Section_650a105f64434eb0839a188708328fb0) | The NetrLogonControl2 method executes a specific Netlogon control operation. This method extends NetrLogonControl by allowing an input buffer that contains data for a particular query.  Opnum: 14 |
| [NetrServerAuthenticate2](#Section_985982ae9aa84565b30b33d6353d3355) | The NetrServerAuthenticate2 method handles logoff requests for the Security Account Manager (SAM).  Opnum: 15 |
| [NetrDatabaseSync2](#Section_31fc80bd4f4d4512a792e488bb78f6a0) | The NetrDatabaseSync2 method is used by a BDC to request the entire [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) from a PDC. It can be called only by a BDC that has been previously authenticated by the PDC.  Opnum: 16 |
| [NetrDatabaseRedo](#Section_c8352ce88b094baeaaf7456d7e6fda6c) | The NetrDatabaseRedo method is used by a SAM BDC to request information about a single account. It can be called only by a BDC that has been previously authenticated by the PDC.  Opnum: 17 |
| [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) | The NetrLogonControl2Ex method executes a specific Netlogon control operation. The introduction of this method added support for query level (4) to both NetrLogonControl2Ex and NetrLogonControl2 for retrieving user account information.  Opnum: 18 |
| [NetrEnumerateTrustedDomains](#Section_1d106b28c30f4fd1b7b0240b6250d7f6) | The NetrEnumerateTrustedDomains method returns an enumeration of [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain names**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c).  Opnum: 19 |
| [DsrGetDcName](#Section_86a3fa5b1f0e412a942f33a10e5e9eff) | The DsrGetDcName method returns the current domain controller for a specified domain.  Opnum: 20 |
| [NetrLogonGetCapabilities](#Section_5780fc6c82f0489fb9a0a9e855388492) | The NetrLogonGetCapabilities method returns server capabilities.  Opnum: 21 |
| [NetrLogonSetServiceBits](#Section_481bb1f8319a40fb89cdad1f6a146d9d) | The NetrLogonSetServiceBits method indicates to Netlogon whether a domain controller is running a specified service. This is done by setting service bits.  Opnum: 22 |
| [NetrLogonGetTrustRid](#Section_1d6fad9e763d495f9bed18c79304c3d7) | The NetrLogonGetTrustRid method is used to obtain the [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the account that is used by the specified server in its [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca), to determine the **DomainName** for the specified domain.  Opnum: 23 |
| [NetrLogonComputeServerDigest](#Section_5f95c374795142d9816cc7f4cff2ed52) | The NetrLogonComputeServerDigest method computes a cryptographic digest of a message.  Opnum: 24 |
| [NetrLogonComputeClientDigest](#Section_79ca6e90ccd2429eb5ac8050b620eef6) | The NetrLogonComputeClientDigest method is used by a client to compute a cryptographic digest of a message.  Opnum: 25 |
| [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) | The NetrServerAuthenticate3 method extends NetrServerAuthenticate2, returning an account RID after authentication.  Opnum: 26 |
| [DsrGetDcNameEx](#Section_5de19b7e4ce34cc4978f8959f46797ba) | The DsrGetDcNameEx method returns the current domain controller for a specified domain and [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba).  Opnum: 27 |
| [DsrGetSiteName](#Section_2b0173e28c454fde8967ad1cbbc7e593) | The DsrGetSiteName method returns the site name for a specified computer.  Opnum: 28 |
| [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) | The NetrLogonGetDomainInfo method returns information that describes the current domain to which a specified client belongs.  Opnum: 29 |
| [NetrServerPasswordSet2](#Section_14b020a80bcf4af5ab72cc92bc6b1d81) | The NetrServerPasswordSet2 method allows an account to set a new clear text password. This method extends NetrServerPasswordSet, which specifies an encrypted [**one-way function (OWF)**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of a password.  Opnum: 30 |
| [NetrServerPasswordGet](#Section_5647a125f6ae4ea6acec14f3e9ec3a8b) | The NetrServerPasswordGet method allows a BDC to get a computer account password from the PDC in the domain.  Opnum: 31 |
| [NetrLogonSendToSam](#Section_b06e6b30fe574e0fba1a5214c953a5df) | The NetrLogonSendToSam method allows a BDC or [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to forward user account password changes to the PDC.  Opnum: 32 |
| [DsrAddressToSiteNamesW](#Section_0731ce2efde2405cb7d7c9012df9d718) | The DsrAddressToSiteNamesW method resolves a list of socket addresses as their corresponding site names.  Opnum: 33 |
| [DsrGetDcNameEx2](#Section_fb8e1146a0454c3198d1c68507ad5620) | The DsrGetDcNameEx2 method returns the current DC for a specified domain and site.  Opnum: 34 |
| [NetrLogonGetTimeServiceParentDomain](#Section_be27686c237347439b655c97b2618bdd) | The NetrLogonGetTimeServiceParentDomain method returns the name of the parent domain of the current domain.  Opnum: 35 |
| [NetrEnumerateTrustedDomainsEx](#Section_c3e9870a09434d45be94edb9419a1c11) | The NetrEnumerateTrustedDomainsEx method returns a list of trusted domains from a specified server.  Opnum: 36 |
| [DsrAddressToSiteNamesExW](#Section_95c432063a184af3928d02d2e0c3d6c1) | The DsrAddressToSiteNamesExW method translates a list of socket addresses into their corresponding site names and subnet names.  Opnum: 37 |
| [DsrGetDcSiteCoverageW](#Section_6d26f254b1254f0f84411ca66cc93b2f) | The DsrGetDcSiteCoverageW method returns a list of sites covered by a DC.  Opnum: 38 |
| [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd) | The NetrLogonSamLogonEx method provides an extension to NetrLogonSamLogon that allows for [**NT LAN Manager (NTLM)**](#gt_6e52bc15-d369-45fd-b098-d51fc9baa56a) pass-through authentication.  Opnum: 39 |
| [DsrEnumerateDomainTrusts](#Section_f98236242b34415cbdca9f9a6d97016b) | The DsrEnumerateDomainTrusts method returns an enumerated list of domain trusts, filtered by a set of flags, from a specified server.  Opnum: 40 |
| [DsrDeregisterDnsHostRecords](#Section_db6c9aad573640c5af86538dd439134c) | The DsrDeregisterDnsHostRecords method deletes [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) entries, except for type A records registered by a DC.  Opnum: 41 |
| [NetrServerTrustPasswordsGet](#Section_84b0d22a9b2c44328ae04a72eda28ea4) | The NetrServerTrustPasswordsGet method returns encrypted passwords for an account on a server.  Opnum: 42 |
| [DsrGetForestTrustInformation](#Section_8bff4d0be06c4c3a8bd9b0e2a7f2b06b) | The DsrGetForestTrustInformation method retrieves the trust information for the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) of the specified domain controller, or for a forest trusted by the forest of the specified DC.  Opnum: 43 |
| [NetrGetForestTrustInformation](#Section_63bab11ca90244a29cd7221357788483) | The NetrGetForestTrustInformation method retrieves the trust information for the forest of which the member's domain is itself a member.  Opnum: 44 |
| [NetrLogonSamLogonWithFlags](#Section_d17f1077de4b4fcd886739068cb789f5) | The NetrLogonSamLogonWithFlags method handles logon requests for the SAM according to specific property flags.  Opnum: 45 |
| [NetrServerGetTrustInfo](#Section_4c2296c3c6f047fc9f01a6fe17bf1d5b) | The NetrServerGetTrustInfo method returns an information block from a specified server. The information includes encrypted passwords for a particular account and trust data.  Opnum: 46 |
| OpnumUnused47 | Opnum: 47 |
| [DsrUpdateReadOnlyServerDnsRecords](#Section_e83df1615c134520ae5a79218ed0bb19) | The DsrUpdateReadOnlyServerDnsRecords method allows an RODC to send a control command to a normal (writable) DC for site-specific and CName types of DNS records update.  Opnum: 48 |
| [NetrChainSetClientAttributes](#Section_3a416e8202994ff0a25d223f972ba1d6) | When a read-only DC receives either the NetrServerAuthenticate3 method or the NetrLogonGetDomainInfo method, with updates requested, it invokes this method on a normal (writable) DC to update to a client's computer account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90).  Opnum: 49 |

**Note** that gaps in the [**opnum**](#gt_e127848e-c66d-427d-b3aa-9f904fa4ada7) numbering sequence represent opnums that SHOULD NOT[<143>](#Appendix_A_143" \o "Product behavior note 143) be used over the wire.

All methods MUST NOT throw an exception.

The following is a complete list of the Netlogon methods that require a secure channel to be established before they are called by a client. See section [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9) for details about how to establish a secure channel between the client and the server:

* DsrUpdateReadOnlyServerDnsRecords
* NetrGetForestTrustInformation
* NetrLogonSamLogon
* NetrLogonSamLogonEx
* NetrLogonSamLogonWithFlags
* NetrLogonSamLogoff
* NetrLogonSendToSam
* NetrServerPasswordGet
* NetrServerPasswordSet
* NetrServerPasswordSet2
* NetrServerGetTrustInfo
* NetrServerTrustPasswordsGet
* NetrLogonGetDomainInfo
* NetrChainSetClientAttributes
* NetrDatabaseDeltas
* NetrDatabaseSync
* NetrDatabaseSync2
* NetrDatabaseRedo
* NetrAccountDeltas
* NetrAccountSync
* NetrLogonDummyRoutine1

#### RPC Binding Handles for Netlogon Methods

[**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) binding is the process of creating a logical connection between a client and a server. The information that composes the binding between client and server is represented by a structure called a [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed).

All Netlogon RPC methods accept an RPC binding handle as the first parameter. With the exception of the [NetrLogonSamLogonEx (section 3.5.4.5.1)](#Section_1725735133844de5bfe0453926ef67cd) method, which uses an RPC primitive binding handle (see [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.2.3.1), all Netlogon RPC methods use a custom binding handle.

This type is declared as follows:

1. typedef [handle] wchar\_t\* LOGONSRV\_HANDLE;

This custom binding handle is a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string of the name of the server that receives the call. The server name can be in either the NetBIOS format or the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) format. It might or might not be prefixed with two backslashes. There is no prescriptive requirement regarding backslashes. If the string is NULL, the server is the same as the client (that is, the local computer).

#### Determining client privileges

To determine access rights, the client access token is retrieved from the [**RPC transport**](#gt_c2eeb200-3cd0-4916-966e-d7d6bff1737a), as described for RpcImpersonationAccessToken in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.3.4.3.

Method Access Control Algorithm: During processing of methods that implement access checks, the server implementing this protocol SHOULD perform access security verification on the client's identity, using the algorithm specified by the Access Check Algorithm Pseudo code ([[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.5.3.2). For this protocol, the input parameters of that algorithm are mapped as follows:

* *SecurityDescriptor*: This MUST be the NetlogonSecurityDescriptor ADM element.
* *Token / Authorization Context*: This MUST be the identity of the client from the ADM element RpcImpersonationAccessToken, retrieved as specified in [MS-RPCE] section 3.3.3.4.3.
* *Access Request mask*: This is specified by each method's processing logic and MUST be one or more of the Access Rights specified previously in section [2.2.1.4.18](#Section_b698c4175da343b9a603eb1d4bd1cb77).
* *Object Tree*: This parameter MUST be NULL.
* *PrincipalSelfSubst SID*: This parameter MUST be NULL.

#### DC Location Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used to locate a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### DsrGetDcNameEx2 (Opnum 34)

The DsrGetDcNameEx2 method SHOULD[<144>](#Appendix_A_144" \o "Product behavior note 144) return information about a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) and [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba). If the *AccountName* parameter is not NULL, and a DC matching the requested capabilities (as defined in the *Flags* parameter) responds during this method call, then that DC will have verified that the DC account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) contains an account for the *AccountName* specified. The server that receives this call is not required to be a DC.

1. NET\_API\_STATUS DsrGetDcNameEx2(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [in, unique, string] wchar\_t\* AccountName,
4. [in] ULONG AllowableAccountControlBits,
5. [in, unique, string] wchar\_t\* DomainName,
6. [in, unique] GUID\* DomainGuid,
7. [in, unique, string] wchar\_t\* SiteName,
8. [in] ULONG Flags,
9. [out] PDOMAIN\_CONTROLLER\_INFOW\* DomainControllerInfo
10. );

**ComputerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the account that MUST exist and be enabled on the DC.

**AllowableAccountControlBits:** A set of bit flags that list properties of the *AccountName* account. A flag is TRUE (or set) if its value is equal to 1. If the flag is set, then the account MUST have that property; otherwise, the property is ignored. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | F | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | E | D | C | 0 | B | A | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Account for users whose primary account is in another domain. This account provides user access to the domain, but not to any domain that [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) the domain. |
| B | Normal domain user account. |
| C | Interdomain trust account. |
| D | Computer account for a [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65). |
| E | Computer account for a BDC. |
| F | Computer account for an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870).[<145>](#Appendix_A_145" \o "Product behavior note 145) |

All other bits MUST be set to zero and MUST be ignored on receipt.

**DomainName:** A null-terminated Unicode string that contains the [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c). If the string is NULL or empty (that is, the first character in the string is the null-terminator character), then the primary domain name is assumed.

**DomainGuid:** A pointer to a [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) structure that specifies the GUID of the domain queried. If *DomainGuid* is not NULL and the domain specified by *DomainName* cannot be found, the DC locator attempts to locate a DC in the domain that has the GUID specified by *DomainGuid*. This allows renamed domains to be found by their GUID.

**SiteName:** A null-terminated string that contains the name of the site in which the DC MUST be located.

**Flags:** A set of bit flags that provide additional data that is used to process the request. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| S | R | 0 | 0 | 0 | 0 | 0 | 0 | W | V | U | T | Q | P | O | N | M | L | K | J | I | H | G | F | E | D | C | B | 0 | 0 | 0 | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | The server ignores any cached DC data. |
| B | The server returns a DC that supports [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e) functions. |
| C | The server first attempts to find a DC that supports directory service functions. |
| D | The server returns a DC that is a [**global catalog**](#gt_4f5d605a-7b3f-4db7-8c21-b146856d7169) server for the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). |
| E | The server returns a DC that is the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) for the domain. |
| F | The server uses cached DC data if available, even if the cached data is expired. |
| G | The server returns a DC that has an IP (either IPv4 or IPv6) address. |
| H | The server returns a DC that is currently running the Kerberos [**Key Distribution Center**](#gt_6e5aafba-6b66-4fdd-872e-844f142af287) service. |
| I | The server returns a DC that is currently running [**W32Time**](#gt_43e51d0a-ac6a-4662-a99a-8f3029b78caf). |
| J | The server returns a DC that is writable. |
| K | The server first attempts to find a DC that is a reliable time server. If a reliable time server is unavailable, the server returns a DC that is currently running W32Time. |
| L | The server returns a different DC in the domain, if one exists. |
| M | The server returns a server that is an LDAP server. The server MAY return a DC. |
| N | Specifies that the *DomainName* parameter is a [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf). |
| O | Specifies that the *DomainName* parameter is a [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) name. |
| P | The server attempts to find a DC in the next closest site, if a DC in the closest site is not available. If a DC in the next closest site is also not available, the server returns any available DC.[<146>](#Appendix_A_146" \o "Product behavior note 146) |
| Q | The server returns a DC that has a DC functional level of DS\_BEHAVIOR\_WIN2008 or greater, as specified in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.4.2. |
| R | Specifies that the names returned in the **DomainControllerName** and **DomainName** fields of *DomainControllerInfo* are DNS names. |
| S | Specifies that the names returned in the **DomainControllerName** and **DomainName** fields of *DomainControllerInfo* are NetBIOS names. |
| T | The server returns a DC that is currently running the Active Directory Web Service. |
| U | The server returns a DC that has a DC functional level of DS\_BEHAVIOR\_WIN2012 or greater, as specified in [MS-ADTS] section 6.1.4.2. |
| V | The server returns a DC that has a DC functional level of DS\_BEHAVIOR\_WIN2012R2 or greater, as specified in [MS-ADTS] section 6.1.4.2. |
| W | The server returns a DC that has a DC functional level of DS\_BEHAVIOR\_WIN2016 or greater, as specified in [MS-ADTS] section 6.1.4.2. |

All other bits MUST be set to zero. The server MUST return ERROR\_INVALID\_FLAGS if any of the unspecified bits are not zero.

**DomainControllerInfo:** A pointer to a [DOMAIN\_CONTROLLER\_INFOW](#Section_9b85a7a48d344b9e9500bf8644ebfc06) structure (section 2.2.1.2.1) containing data about the DC.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following *Flags* parameter validations:

* Flags D, E, and H MUST NOT be combined with each other.
* Flag N MUST NOT be combined with the O flag.
* Flag R MUST NOT be combined with the S flag.
* Flags B, Q, U, V, and W MUST NOT be combined with each other.
* Flag K MUST NOT be combined with any of the flags: B, C, D, E, or H.
* Flag P MUST NOT be set when the SiteName parameter is provided.

The server MUST return ERROR\_INVALID\_FLAGS for any of the previously mentioned conflicting combinations.

Additionally, the server MUST perform the following parameter validations:

* If the flag D is set and *DomainName* parameter is neither NULL nor empty, the *DomainName* is a valid NetBIOS name format or a [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e) format, and the *DomainName* is not the FQDN (1) or NetBIOS name of a trusted forest, then the server MUST return ERROR\_NO\_SUCH\_DOMAIN. To determine the list of trusted forests, and their FQDN) and NetBIOS names, the server MUST use the **TrustedDomains** ADM. The domains from this collection that have the C bit set in the *Flags* field represent the trusted forests.
* If the flag N is set and *DomainName* parameter is neither NULL nor empty and the *DomainName* is NOT a valid NetBIOS name format, then the server MUST return ERROR\_INVALID\_DOMAINNAME.
* If the flag O is set and *DomainName* parameter is neither NULL nor empty and the *DomainName* is NOT in a valid FQDN format and **AllowDnsSuffixSearch** is FALSE, then the server MUST return ERROR\_INVALID\_DOMAINNAME.
* If neither the N flag nor the O flag are specified and *DomainName* parameter is neither NULL nor empty, then the server MUST return ERROR\_INVALID\_DOMAINNAME if the *DomainName* is neither a valid NetBIOS name format nor a valid FQDN format.

If the A bit in *Flags* is not set, then the server SHOULD attempt to use the **LocatedDCsCache** and **FailedDiscoveryCache** if it has them, even if the F bit in *Flags* is not set. The process for this is as follows:

* If there is no entry for the requested domain in **LocatedDCsCache**, then check if it exists in **FailedDiscoveryCache**. If an entry is found in **FailedDiscoveryCache**, then find the [**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e) between the current time and the last failure time for that cache entry. If this delta is less than **FailedDiscoveryCachePeriod**, the server SHOULD return an error.
* If there is an entry for the requested domain in **LocatedDCsCache**, but its capabilities do not include the requested capabilities, then invalidate the cached entry and attempt to locate a DC as described below.
* If the delta between the current time and the creation time for the entry in **LocatedDCsCache** is greater than the **CacheEntryValidityPeriod** and the F bit in the *Flags* is not set, then invalidate the cached entry and attempt to locate a DC as described below.
* If the difference between the current time and the refresh time for the entry in **LocatedDCsCache** is greater than **CacheEntryPingValidityPeriod**, then the server MUST send a ping message to the DC prior to returning the value. The ping mechanism to be used, whether LDAP Ping ([MS-ADTS] section 6.3.3) or Mailslot Ping ([MS-ADTS] section 6.3.5), is determined based on the N and O bit settings in the *Flags*, as described below. If a ping of the DC fails, then it MUST invalidate the cache entry and attempt to locate a DC as described below. Otherwise update the refresh time and return the cached result.

The server MUST attempt to locate a domain controller for the domain specified by the client. The server SHOULD[<147>](#Appendix_A_147" \o "Product behavior note 147) implement alternate means of locating a DC: for example, a static list in a file, or the two methods detailed in [MS-ADTS] section 6.3.6.

If the *ComputerName* parameter is not NULL, it is compared against the server's [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b). If the server is not a DC (section [3.1.4.8](#Section_16f8294280d643ac8c38eee3cfe4ac99)) and the *ComputerName* parameter does not match the server's computer name, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME. If the *ComputerName* parameter matches the server's computer name, the *ComputerName* parameter is NULL, or the server is a DC, then processing proceeds.

The server can use the DC location protocol ([MS-ADTS] section 6.3.6) to locate a DC (the located DC is known as the responding DC). There are two methods of locating a DC that the DC location protocol supports. One of the methods involves the DNS-based discovery mechanism (described below) and then the LDAP ping message, and the other method involves the [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) ping message.

If the N bit is set in the *Flags* parameter, the mailslot message MUST be sent.

If the O bit is set in the *Flags* parameter, DNS-based discovery MUST be performed and the LDAP message MUST be sent.

* If the *DomainName* parameter is an FQDN with a single label and **AllowDnsSuffixSearch** is TRUE and **AllowSingleLabelDNSDomain** is FALSE, then a DNS-based discovery SHOULD be attempted. The DNS SRV queries specified below SHOULD be performed by using FQDNs formed by appending in turn each of the server's DNS suffixes to *DomainName*.

If neither the N bit nor the O bit are specified, then:

* If the *DomainName* parameter is an FQDN with more than one label (as specified in [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264)), or if the **AllowSingleLabelDNSDomain** field is TRUE and the *DomainName* parameter is an FQDN with a single label, then a DNS-based discovery SHOULD be attempted and an LDAP message SHOULD be sent.
* If the DomainName parameter is a syntactically valid NetBIOS name (as specified in [[MS-NBTE]](%5bMS-NBTE%5d.pdf#Section_3461cfa83d284fa38163131bf1046fa3)), then the mailslot message MUST be sent.

If the DNS-based discovery is performed, the server identifies the candidate DCs by performing DNS SRV queries as follows:

1. Based on the value of the B, D, E, H, and M bits in the *Flags* parameter, the appropriate query is selected from those listed in [MS-ADTS] section 6.3.6. Other bits specified in the *Flags* parameter do not contribute to the selection of this query but are used to validate against the capabilities published in the ping response. The table below shows the specific query that is used for the different valid combinations of these bits:

| Bits specified | Non site-specific query | Site-specific query |
| --- | --- | --- |
| B=0/1, D=0, E=1, H=0, M=0/1 | \_ldap.\_tcp.pdc.\_msdcs.<domainname> | N/A |
| B=0/1, D=0, E=0, H=1, M=0/1 | \_kerberos.\_tcp.dc.\_msdcs.<domainname> | \_kerberos.\_tcp.<sitename>.\_sites.dc.\_msdcs.<domainname> |
| B=0/1, D=1, E=0, H=0, M=1 | \_gc.\_tcp.<forestname> | \_gc.\_tcp.<sitename>.\_sites.<forestname> |
| B=0/1, D=0, E=0, H=0, M=1 | \_ldap.\_tcp.<domainname> | \_ldap.\_tcp.<sitename>.\_sites.<domainname> |
| B=0/1, D=1, E=0, H=0, M=0 | \_gc.\_tcp.dc.\_msdcs.<forestname> | \_gc.\_tcp.<sitename>.\_sites.dc.\_msdcs.<forestname> |
| B=0/1, D=0, E=0, H=0, M=0 | \_ldap.\_tcp.dc.\_msdcs.<domainname> | \_ldap.\_tcp.<sitename>.\_sites.dc.\_msdcs.<domainname> |

1. If the SiteName parameter is not NULL, the server MUST attempt a site-specific query. For example, if the request is to locate a Key Distribution Center (KDC), the following query is used: \_kerberos.\_tcp.<*SiteName*>.\_sites.dc.\_msdcs.<*DomainName*>.
2. If the *SiteName* parameter is NULL, the server MUST attempt to first use a site-specific query for the **SiteName** (ADM element) site where applicable. For example, if the request is to locate a KDC, the following query is used: \_kerberos.\_tcp.<**SiteName**>.\_sites.dc.\_msdcs.<*DomainName*>. If the site-specific query does not result in any candidate domain controllers, or if the candidate domain controllers are not reachable via LDAP ping (described below), and if the P bit in the *Flags* parameter is set, and if **NextClosestSiteName** (ADM element) is not NULL, then the server MUST attempt to locate a DC in the next closest site by performing a site-specific query for **NextClosestSiteName**. If a DC in the next closest site is not available, or if the P bit in the *Flags* parameter was not set, or if **NextClosestSiteName** was NULL, the server MUST return any available DC, using a non-site-specific query to determine the candidate domain controllers. Using the same KDC example as before, the following non-site-specific query is used: \_kerberos.\_tcp.dc.\_mcdcs.<*DomainName*>.

In either mechanism (described in [MS-ADTS] section 6.3.6), multiple candidate DCs can be discovered. The candidate DCs are pinged to determine availability and ability to satisfy the specified requirements.

The LDAP/mailslot ping messages are constructed as follows:

When using the LDAP ping method ([MS-ADTS] section 6.3.3), the server MUST set the parameters of the LDAP message as follows:

* The **DnsDomain** field of the message is set to the *DomainName* parameter of the **DsrGetDcNameEx2** call. If *DomainName* is NULL, the **DnsDomain** field of the message is set to **DnsDomainName** (section [3.5.1](#Section_b8d168acebb642f4bfb27a84377f2cbc)). If the *DomainName* parameter is an FQDN with a single label and **AllowDnsSuffixSearch** is TRUE and **AllowSingleLabelDNSDomain** is FALSE, the **DnsDomain** field of the message is set to the FQDN (2) formed by appending in turn each of the server's DNS suffixes to *DomainName*.
* The **Host** field of the message is set to the *ComputerName* that is sending the message.
* The **User** field of the message is not set.
* The **AAC** field of the message is not set.
* The **DomainSid** field of the message is not set.
* If the **DomainGuid** parameter of the **DsrGetDcNameEx2** is not NULL, the **DomainGuid** field of the message is set to the *DomainGuid* parameter, else the **DomainGuid** field of the message is not set.

When using the mailslot ping method ([MS-ADTS] section 6.3.5), the server MUST set the parameters of the mailslot message as follows:

* The **UnicodeComputerName** field of the message is set to the *ComputerName* that is sending the message.
* The **UnicodeUserName** field of the message is not set.
* The **AllowableAccountControlBits** field of the message is not set.
* The **DomainSidSize** field of the message is set to 0x00000000.
* The **DomainSid** field of the message is not set.
* The **DomainGuid** field of the message is not set.

If the *AccountName* parameter is specified, the server MUST perform the following additional processing that is described in detail in [MS-ADTS]:

* The LDAP and mailslot query message fields are set as specified in [MS-ADTS] sections 6.3.3 and 6.3.5, except for the following:
  + LDAP ping message:
    - The **User** field of the message is set to the value of the *AccountName* parameter.
    - The **AAC** field of the message is mapped from the *AllowableAccountControlBits* parameter, according to the table in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 3.1.5.14.2, where the "ProtocolUserAccountControl" column defines the **AAC** field while the "DatabaseUserAccountControl" column defines the *AllowableAccountControlBits*.
  + Mailslot message:
    - The **UnicodeUserName** field of the message is set to the value of the *AccountName* parameter.
    - The **AllowableAccountControlBits** field of the message is mapped from the *AllowableAccountControlBits* parameter, according to the table in [MS-SAMR] section 3.1.5.14.2, where the "ProtocolUserAccountControl" column defines the **AAC** field while the "DatabaseUserAccountControl" column defines the *AllowableAccountControlBits*.

LDAP/Mailslot ping responses from the candidate DCs are processed (in the order in which they are received) along with the flags to determine if the server queried meets all of the requirements, until a server that meets the requirements is found or an implementation-specific timeout is reached.

If the B bit in the *Flags* is set, the server SHOULD[<148>](#Appendix_A_148" \o "Product behavior note 148) return a DC that supports directory service functions. To determine if a domain controller meets this requirement, the server MUST check the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE.NtVersion** field in the message and ensure that NETLOGON\_NT\_VERSION\_5 or greater is specified. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the C bit in the *Flags* is set, the service MUST first attempt to find a DC that supports directory service functions.[<149>](#Appendix_A_149" \o "Product behavior note 149) To determine if a domain controller meets this requirement, the server MUST check the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE.NtVersion** field in the message and ensure that NETLOGON\_NT\_VERSION\_5 or greater is specified. If a DC that supports the directory service functions is not available, the server MUST return the name of a non–directory service DC.

If the D bit in the *Flags* is set, the server MUST return a DC that is a global catalog server for the forest of domains. To determine if a domain controller is a global catalog server, the server MUST check the value of the FG bit in the *Flags* field of the message as defined in [MS-ADTS] section 6.3.1.2.

If the E bit in the *Flags* is set, the server MUST return a DC that is the PDC for the domain. To determine if a domain controller is a primary domain controller the server MUST check the value of the FP bit in the *Flags* field of the message as defined in [MS-ADTS] section 6.3.1.2. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the G bit in the *Flags* is set, the server MUST return a DC that has an IP (either IPv4 or IPv6) address. The IP address can be verified by examining the **DcIpAddress** field of the NETLOGON\_SAM\_LOGON\_RESPONSE message ([MS-ADTS] section 6.3.1.8) or the **DcSockAddr** field of the NETLOGON\_SAM\_LOGON\_RESPONSE\_EX message ([MS-ADTS] section 6.3.1.9). If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the H bit in the *Flags* is set, the server MUST return a DC that is currently running the Kerberos Key Distribution Center service. To determine if a domain controller is currently running the Kerberos Key Distribution Center service, the server MUST check the value of the FK bit in the **Flags** field of the message as defined in [MS-ADTS] section 6.3.1.2. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the I bit in the *Flags* is set, then the server MUST return a DC that is currently running W32Time. To determine if a domain controller is currently running an [[MS-SNTP]](%5bMS-SNTP%5d.pdf#Section_8106cb73ab3a45428bc8784dd32031cc) implementation, the server MUST check the value of the FT bit in the *Flags* field of the message as defined in [MS-ADTS] section 6.3.1.2. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the J bit in the *Flags* is set, the server MUST return a DC that is writable.[<150>](#Appendix_A_150" \o "Product behavior note 150) To determine if a domain controller is writable, the server MUST check the value of the FW bit in the *Flags* field of the message as defined in [MS-ADTS] section 6.3.1.2. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the K bit in the *Flags* is set, the server returns a DC that is a reliable time server. If a reliable time server is unavailable, the server returns a DC that is a time server. To determine whether a domain controller is a reliable time server, the server MUST check the value of the FGT bit in the **Flags** field of the message as defined in [MS-ADTS] section 6.3.1.2. To determine whether a domain controller is a time server, the server MUST check the value of the FT bit in the **Flags** field of the message as defined in [MS-ADTS] section 6.3.1.2. If a domain controller that meets either of these requirements cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the L bit in the **Flags** is set, the server MUST return a DC in the domain other than the server, if one exists. This flag is ignored if the recipient if not running as a DC.

If the M bit in the *Flags* is set, the server MUST return an LDAP server. To determine if a domain controller is an LDAP server, the server MUST check the value of the FL bit in the **Flags** field of the message as defined in [MS-ADTS] section 6.3.1.2. The server MAY return a DC. No other services are required to be present on the server returned. The server MAY return a server that has a writable config container or a writable schema container. If the D bit in the **Flags** is set, the server returned MUST be an LDAP server and a global catalog server, and might be a DC. No other services are implied to be present at the server. If this flag is specified, the B, C, E, H, I, J, and T bits in the **Flags** are ignored along with their respective processing requirements.

If the Q bit in **Flags** is set, the server MUST return a DC that has a functional level of DS\_BEHAVIOR\_WIN2008 or greater. To determine the functional level of a DC, the server MUST locate the DC's nTDSDSA object in the directory and verify the **msDS-Behavior-Version** attribute as specified in [MS-ADTS] section 6.1.4.2.

If the T bit in the *Flags* is set, the server SHOULD[<151>](#Appendix_A_151" \o "Product behavior note 151) return a DC that is currently running the Active Directory Web Service. To determine if a domain controller is currently running the Active Directory Web Service, the server MUST check the value of the FWS bit in the *Flags* field of the message as defined in [MS-ADTS] section 6.3.1.2. If a server that meets this requirement cannot be located, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the U bit in **Flags** is set, the server MUST return a DC that has a functional level of DS\_BEHAVIOR\_WIN2012 or greater. To determine the functional level of a DC, the server MUST locate the DC's nTDSDSA object in the directory and verify the **msDS-Behavior-Version** attribute as specified in [MS-ADTS] section 6.1.4.2.

If the V bit in **Flags** is set, the server MUST return a DC that has a functional level of DS\_BEHAVIOR\_WIN2012R2 or greater. To determine the functional level of a DC, the server MUST locate the DC's nTDSDSA object in the directory and verify the **msDS-Behavior-Version** attribute as specified in [MS-ADTS] section 6.1.4.2.

If the W bit in **Flags** is set, then the server MUST return a DC that has a functional level of DS\_BEHAVIOR\_WIN2016 or greater. To determine the functional level of a DC, the server MUST locate the DC's nTDSDSA object in the directory and verify the **msDS-Behavior-Version** attribute as specified in [MS-ADTS] section 6.1.4.2.

NETLOGON\_SAM\_LOGON\_RESPONSE\_EX ([MS-ADTS] section 6.3.1.9) and NETLOGON\_SAM\_LOGON\_RESPONSE ([MS-ADTS] section 6.3.1.8) messages are received from a DC in response to the LDAP and the mailslot messages, respectively. Using these response messages, the **DsrGetDcNameEx2** populates the returned DOMAIN\_CONTROLLER\_INFOW structure (section 2.2.1.2.1) as follows:

* The **DnsHostName**, **DnsDomainName**, **NetbiosComputerName**, and **NetbiosDomainName** fields are compressed and MUST be decompressed as described in [MS-ADTS] section 6.3.7.
* If the R flag is set in the *Flags* parameter:
  + The **DomainControllerInfo.DomainControllerName** field MUST be set to the value of the **DnsHostName** message field. If the **DnsHostName** field is not set in the message, the error ERROR\_NO\_SUCH\_DOMAIN MUST be returned.
  + The **DomainControllerInfo.DomainName** field MUST be set to the value of the **DnsDomainName** message field. If the **DnsDomainName** field is not set in the message, the error ERROR\_NO\_SUCH\_DOMAIN MUST be returned.
* If the S flag is set in the *Flags* parameter:
  + The **DomainControllerInfo.DomainControllerName** field MUST be set to the value of the **NetbiosComputerName** message field.
  + The **DomainControllerInfo.DomainName** field MUST be set to the value of the **NetbiosDomainName** message field.
* If neither the R nor S flags are set in the *Flags* parameter:[<152>](#Appendix_A_152" \o "Product behavior note 152)
  + The **DomainControllerInfo.DomainControllerName** field MUST be set to either the value of the **DnsHostName** message field, or to the value of the **NetbiosComputerName** message field.[<153>](#Appendix_A_153" \o "Product behavior note 153)
  + The **DomainControllerInfo.DomainName** field MUST be set to either the value of the **DnsDomainName** message field, or to the value of the **NetbiosDomainName** message field.[<154>](#Appendix_A_154" \o "Product behavior note 154)
* If the IP address of the DC to which the message was sent is known from the underlying transport protocol, the **DomainControllerInfo.DomainControllerAddress** field MUST be set to that address. Otherwise, the field SHOULD be set from the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DcSockAddr** message field if the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DcSockAddrSize** message field is not zero.
* If the IP address of the DC is not available because the aforementioned conditions are not met, the **DomainControllerInfo.DomainControllerAddress** field MUST be set to the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.NetbiosComputerName** field.
* The **DomainControllerInfo.DomainControllerAddressType** field MUST be set to 0x00000001 if the **DomainControllerAddress** field is set to the IP address of the DC. Otherwise, the **DomainControllerInfo.DomainControllerAddressType** field MUST be set to 0x00000002 for a NETBIOS name.
* The **DomainControllerInfo.DomainGuid** field MUST be set to the **NETLOGON\_SAM\_LOGON\_RESPONSE.DomainGuid** or the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DomainGuid** field.
* The **DomainControllerInfo.DnsForestName** field MUST be set to the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE.DnsForestName** or the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DnsForestName** fields if they are present, or to NULL if the **NETLOGON\_SAM\_LOGON\_RESPONSE.DnsForestName** and the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DnsForestName** fields are not present.
* The **DomainControllerInfo.Flags** field MUST be set to the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE.Flags** or the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.Flags** field. Additionally, the following flags are set in the **DomainControllerInfo.Flags** field:
  + The flag M MUST be set if the **DomainControllerInfo.DomainControllerName** field is set to the FQDN (1) of the DC.
  + The flag N MUST be set if the **DomainControllerInfo.DomainName** field is set to the FQDN (1) of the domain.
  + The flag O MUST be set if the **DomainControllerInfo.DnsForestName** field is set.
* The **DomainControllerInfo.DcSiteName** field MUST be set to the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DcSiteName** field if it is present, or to NULL if the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.DcSiteName** field is not present.
* The **DomainControllerInfo.ClientSiteName** field MUST be set to the value of the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.ClientSiteName** field if it is present, or to NULL if the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.ClientSiteName** field is not present.
  + If the **NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.NextClosestSiteName** field is present, the value MUST be saved in the **NextClosestSiteName** ADM element.

If a satisfactory NETLOGON\_SAM\_LOGON\_RESPONSE\_NT40 ([MS-ADTS] section 6.3.1.7) response message is received from a Windows NT 4.0 DC in response to the mailslot messages, the **DsrGetDcNameEx2** call populates the returned **DOMAIN\_CONTROLLER\_INFOW** structure (section 2.2.1.2.1) as follows:

* The **DomainControllerInfo.DomainControllerName** field MUST be set to the **NETLOGON\_SAM\_LOGON\_RESPONSE\_NT40.UnicodeLogonServer** field.
* The **DomainControllerInfo.DomainControllerAddress** field MUST be set to the **NETLOGON\_SAM\_LOGON\_RESPONSE\_NT40.UnicodeLogonServer** field.
* The **DomainControllerInfo.DomainControllerAddressType** field MUST be set to 0x00000002.
* The **DomainControllerInfo.DomainGuid** field MUST be set to NULL.
* The **DomainControllerInfo.DomainName** field MUST be set to the **NETLOGON\_SAM\_LOGON\_RESPONSE\_NT40.UnicodeLogonServer** field.
* The **DomainControllerInfo.DnsForestName** field MUST be set to NULL.
* The **DomainControllerInfo.Flags** field MUST have the A and H flags set if the response is to a PDC query; otherwise it MUST be set to 0x00000000.
* The **DomainControllerInfo.DcSiteName** field MUST be set to NULL.
* The **DomainControllerInfo.ClientSiteName** field MUST be set to NULL.

If the *AccountName* parameter is not NULL, the response message validation adds the following check: if the DC response is received indicating the lack of an account, as specified in [MS-ADTS] sections 6.3.3 and 6.3.5, the server MUST return ERROR\_NO\_SUCH\_USER.

If the server successfully locates a DC for the requested capabilities, then it SHOULD save the result in the **LocatedDCsCache**. If a DC for the domain cannot be located, then the server SHOULD save the result in the **FailedDiscoveryCache**.

##### DsrGetDcNameEx (Opnum 27)

The DsrGetDcNameEx method is a predecessor to the [DsrGetDcNameEx2 (section 3.5.4.3.1)](#Section_fb8e1146a0454c3198d1c68507ad5620) method. The method SHOULD[<155>](#Appendix_A_155" \o "Product behavior note 155) return information about a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) and [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba). All parameters of this method have the same meanings as the identically named parameters of the DsrGetDcNameEx2 method.

1. NET\_API\_STATUS DsrGetDcNameEx(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [in, unique, string] wchar\_t\* DomainName,
4. [in, unique] GUID\* DomainGuid,
5. [in, unique, string] wchar\_t\* SiteName,
6. [in] ULONG Flags,
7. [out] PDOMAIN\_CONTROLLER\_INFOW\* DomainControllerInfo
8. );

On receiving this call, the server MUST perform all of the processing done on receiving the **DsrGetDcNameEx2** call, except that any processing specific to the *AccountName* and *AllowableAccountControlBits* parameters is ignored. This function MUST be processed as if the *AccountName* and *AllowableControlBits* parameters were not specified.

##### DsrGetDcName (Opnum 20)

The DsrGetDcName method is a predecessor to the [DsrGetDcNameEx2](#Section_fb8e1146a0454c3198d1c68507ad5620) method (section 3.5.4.3.1). The method SHOULD[<156>](#Appendix_A_156" \o "Product behavior note 156) return information about a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). All parameters of this method have the same meanings as the identically named parameters of the DsrGetDcNameEx2 method, except for the *SiteGuid* parameter, detailed as follows.

1. NET\_API\_STATUS DsrGetDcName(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [in, unique, string] wchar\_t\* DomainName,
4. [in, unique] GUID\* DomainGuid,
5. [in, unique] GUID\* SiteGuid,
6. [in] ULONG Flags,
7. [out] PDOMAIN\_CONTROLLER\_INFOW\* DomainControllerInfo
8. );

**SiteGuid:** This parameter MUST be NULL and ignored upon receipt.

The **DsrGetDcName** call accepts the *SiteGuid* parameter instead of the *SiteName* parameter of the **DsrGetDcNameEx** call. On receiving this call, the server MUST perform all of the processing done on receiving the **DsrGetDcNameEx** call.

##### NetrGetDCName (Opnum 11)

The NetrGetDCName method MAY[<157>](#Appendix_A_157" \o "Product behavior note 157) retrieve the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) for the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. NET\_API\_STATUS NetrGetDCName(
2. [in, string] LOGONSRV\_HANDLE ServerName,
3. [in, unique, string] wchar\_t\* DomainName,
4. [out, string] wchar\_t\*\* Buffer
5. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640), that represents the connection to a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**DomainName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that specifies the NetBIOS name of the domain.

**Buffer:** A pointer to a null-terminated Unicode string that contains the NetBIOS name of the PDC for the specified domain. The server name returned by this method is prefixed by two backslashes (\\).

**Return Values:** The method returns 0x00000000 on success; otherwise, it MUST return a nonzero error code and SHOULD return the following error code.

| Return Value/Code | Description |
| --- | --- |
| 0x00000035  ERROR\_ BAD\_ NETPATH | The network path was not found. |

If the *DomainName* parameter is not NULL and is not a valid NetBIOS name format, the server MUST return NERR\_DCNotFound.

The server MUST attempt to locate a PDC for the domain specified by the client. The server MUST return NERR\_DCNotFound if the PDC could not be located for the specified domain. The server SHOULD[<158>](#Appendix_A_158" \o "Product behavior note 158) implement alternate means of locating DCs: for example, a static list in a file, or two methods detailed in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6.

NetrGetDcName returns the name of the discovered PDC.

##### NetrGetAnyDCName (Opnum 13)

The NetrGetAnyDCName method MAY[<159>](#Appendix_A_159" \o "Product behavior note 159) retrieve the name of a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified primary or directly [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). Only DCs can return the name of a DC in a specified directly trusted domain.

1. NET\_API\_STATUS NetrGetAnyDCName(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, unique, string] wchar\_t\* DomainName,
4. [out, string] wchar\_t\*\* Buffer
5. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**DomainName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the primary or directly trusted domain. If the string is NULL or empty (that is, the first character in the string is the null-terminator character), the primary [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) is assumed.

**Buffer:** A pointer to an allocated buffer that contains the null-terminated Unicode string containing the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of a DC in the specified domain. The DC name is prefixed by two backslashes (\\).

**Return Values:** The method returns 0x00000000 on success; otherwise, it MUST return a nonzero error code and SHOULD return the following error code.

| Return Value/Code | Description |
| --- | --- |
| 0x00000712  ERROR\_DOMAIN\_TRUST\_INCONSISTENT | The name or security ID ([**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d)) of the domain specified is inconsistent with the trust information for that domain. |

The server MUST attempt to locate a DC for the domain specified by the client. The server SHOULD[<160>](#Appendix_A_160" \o "Product behavior note 160) implement alternate means to locate domain controllers: for example, a static list in a file, or the two methods detailed in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6. If the server that receives this call is the PDC for the domain specified in DomainName, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If the *ServerName* parameter is not a valid binding handle (as defined in section 3.5.4.1), the server MUST return ERROR\_INVALID\_COMPUTERNAME.

This method also returns errors based on Common Error Processing Rule E, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

NetrGetAnyDcName returns the name of the discovered DC.

##### DsrGetSiteName (Opnum 28)

The DsrGetSiteName method SHOULD[<161>](#Appendix_A_161" \o "Product behavior note 161) return the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) name for the specified computer that receives this call.

1. NET\_API\_STATUS DsrGetSiteName(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [out, string] wchar\_t\*\* SiteName
4. );

**ComputerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) (defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)).

**SiteName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the site in which the computer that receives this call resides.

**Return Values:** The method returns 0x00000000 on success; otherwise, it MUST return a nonzero error code and SHOULD return the following error code.

| Return Value/Code | Description |
| --- | --- |
| 0x0000077F  ERROR\_NO\_SITENAME | No site name is available for this machine. |

If the computer has been configured with a SiteName, it MUST return the SiteName immediately.

If the DynamicSiteNameSetTime plus the DynamicSiteNameTimeout is less than the current time (meaning that the DynamicSiteNameSetTime is older than allowed by DynamicSiteNameTimeout), then:

* The server MUST locate a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). The server SHOULD[<162>](#Appendix_A_162" \o "Product behavior note 162) implement alternate means to locate DCs: for example, a static list in a file, or the two methods detailed in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.6. If the server cannot locate a DC for the domain, then the server MUST return ERROR\_NO\_SUCH\_DOMAIN.
* The server then populates the *SiteName* parameter with the NETLOGON\_SAM\_LOGON\_RESPONSE\_EX message ([MS-ADTS] section 6.3.1.9) by setting the *SiteName* parameter to NETLOGON\_SAM\_LOGON\_RESPONSE\_EX.ClientSiteName. The server stores the discovered site name in **DynamicSiteName**.
* The server sets the DynamicSiteNameSetTime to the current time.

Otherwise, **DynamicSiteName** MUST be returned immediately as the *SiteName* parameter.

If it is determined that the server that receives this call has no site name, the server MUST return ERROR\_NO\_SITENAME.

This method also returns errors based on Common Error Processing Rules B and C, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

##### DsrGetDcSiteCoverageW (Opnum 38)

The DsrGetDcSiteCoverageW method SHOULD[<163>](#Appendix_A_163" \o "Product behavior note 163) return a list of [**sites**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) covered by a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). Site coverage is detailed in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.1.2.2.

1. NET\_API\_STATUS DsrGetDcSiteCoverageW(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [out] PNL\_SITE\_NAME\_ARRAY\* SiteNames
4. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) (defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)) that represents the connection to a DC.

**SiteNames:** A pointer to an [NL\_SITE\_NAME\_ARRAY](#Section_4c5fb44a6d68420d970e68ad5436bbd3) structure (section 2.2.1.2.2) that contains an array of site name strings.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

This method returns errors based on Common Error Processing Rules A and B, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

The server MUST return all the sites for which the DC publishes site-specific [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) SRV records ([MS-ADTS] section 6.3.2.3).

##### DsrAddressToSiteNamesW (Opnum 33)

The DsrAddressToSiteNamesW method SHOULD[<164>](#Appendix_A_164" \o "Product behavior note 164) translate a list of socket addresses into their corresponding [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) names. For details about the mapping from socket address to subnet/site name, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) sections 6.1.1.2.2.1 and 6.1.1.2.2.2.

1. NET\_API\_STATUS DsrAddressToSiteNamesW(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [in, range(0, 32000)] DWORD EntryCount,
4. [in, size\_is(EntryCount)] PNL\_SOCKET\_ADDRESS SocketAddresses,
5. [out] PNL\_SITE\_NAME\_ARRAY\* SiteNames
6. );

**ComputerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) (section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)) that represents the connection to a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**EntryCount:** The number of socket addresses specified in *SocketAddresses*. The maximum value for *EntryCount* is 32000. The limit was chosen to prevent clients from being able to force large memory allocations on servers.

**SocketAddresses:** An array of [NL\_SOCKET\_ADDRESS](#Section_235d0c09b9db44c59d4d806919be657b) structures (section 2.2.1.2.4) that contains socket addresses to translate. The number of addresses specified MUST be equal to *EntryCount*.

**SiteNames:** A pointer to an [NL\_SITE\_NAME\_ARRAY](#Section_4c5fb44a6d68420d970e68ad5436bbd3) structure (section 2.2.1.2.2) that contains a corresponding array of site names. The number of entries returned is equal to *EntryCount*. The fields of an entry are set to zero if the corresponding socket address does not map to any site, or if the address family of the socket address is not IPV4 or IPV6. The mapping of IP addresses to sites is specified in [MS-ADTS] section 6.1.1.2.2.1.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

| Return Value/Code | Description |
| --- | --- |
| 0x00000008  ERROR\_NOT\_ENOUGH\_MEMORY | Not enough storage is available to process this command. |
| 0x00000057  ERROR\_INVALID\_PARAMETER | One of the parameters is invalid. This error value is returned if the value of *EntryCount* passed to **DsrAddressToSiteNamesW** is zero. |

This method returns errors based on Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

The server MUST return the site names that correspond to the *SocketAddresses* parameter by using the method specified for IP address and site/subnet mapping ([MS-ADTS] section 6.1.1.2.2.2.1).

##### DsrAddressToSiteNamesExW (Opnum 37)

The DsrAddressToSiteNamesExW method SHOULD[<165>](#Appendix_A_165" \o "Product behavior note 165) translate a list of socket addresses into their corresponding [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) names and subnet names. For details about the mapping from socket address to subnet/site name, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) sections 6.1.1.2.2.1 and 6.1.1.2.2.2.

1. NET\_API\_STATUS DsrAddressToSiteNamesExW(
2. [in, unique, string] LOGONSRV\_HANDLE ComputerName,
3. [in, range(0, 32000)] DWORD EntryCount,
4. [in, size\_is(EntryCount)] PNL\_SOCKET\_ADDRESS SocketAddresses,
5. [out] PNL\_SITE\_NAME\_EX\_ARRAY\* SiteNames
6. );

**ComputerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) (defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)) that represents the connection to a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

**EntryCount:** The number of socket addresses specified in *SocketAddresses*. The maximum value for *EntryCount* is 32000. To avoid large memory allocations, this number was chosen as a reasonable limit for the maximum number of socket addresses that this method accepts.

**SocketAddresses:** An array of [NL\_SOCKET\_ADDRESS](#Section_235d0c09b9db44c59d4d806919be657b) structures (section 2.2.1.2.4) that contains socket addresses to translate. The number of addresses specified MUST be equal to *EntryCount*.

**SiteNames:** A pointer to an [NL\_SITE\_NAME\_EX\_ARRAY](#Section_2b40b2eb480c42e9b8643de716db892d) structure (section 2.2.1.2.3) that contains an array of site names and an array of subnet names that correspond to socket addresses in *SocketAddresses*. The number of entries returned is equal to *EntryCount*. The fields of an entry are set to zero if the corresponding socket address does not map to any site, or if the address family of the socket address is not IPV4 or IPV6. The mapping of IP addresses to sites is specified in [MS-ADTS] section 6.1.1.2.2.1.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns one of the following error codes.

| Return Value/Code | Description |
| --- | --- |
| 0x00000008  ERROR\_NOT\_ENOUGH\_MEMORY | Not enough storage is available to process this command. |
| 0x00000057  ERROR\_INVALID\_PARAMETER | One of the parameters is invalid. This error value is returned if the value of *EntryCount* passed to **DsrAddressToSiteNamesExW** is zero. |

This method returns errors based on Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

The server MUST return the site and subnet names that correspond to the *SocketAddresses* by using the method specified for IP address and site/subnet mapping ([MS-ADTS] section 6.1.1.2.2.2.1).

##### DsrDeregisterDnsHostRecords (Opnum 41)

The DsrDeregisterDnsHostRecords method SHOULD[<166>](#Appendix_A_166" \o "Product behavior note 166) delete all of the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) SRV records registered by a specified [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). For the list of SRV records that a [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) registers, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.2.3, "SRV Records Registered by DC".

1. NET\_API\_STATUS DsrDeregisterDnsHostRecords(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, unique, string] wchar\_t\* DnsDomainName,
4. [in, unique] GUID\* DomainGuid,
5. [in, unique] GUID\* DsaGuid,
6. [in, string] wchar\_t\* DnsHostName
7. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640), that represents the connection to the DC.

**DnsDomainName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that specifies the [**FQDN (1)**](#gt_1769aec9-237e-44ed-9014-1abb3ec6de6e).

**DomainGuid:** A pointer to the domain [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1). If the value is not NULL, the DNS SRV record of type \_ldap.\_tcp.DomainGuid.domains.\_msdcs.DnsDomainName is also deregistered.

**DsaGuid:** A pointer to the objectGUID of the DC's NTDSDSA object. For details about the NTDSDSA object, see [MS-ADTS] section 6.1.1.2.2.1.2.1.1. If the value is not NULL, the CNAME [[RFC1035]](https://go.microsoft.com/fwlink/?LinkId=90264) record of the domain in the form of DsaGuid.\_msdcs.DnsDomainName is also deregistered.

**DnsHostName:** A null-terminated Unicode string that specifies the FQDN (1) of the DC whose records are being deregistered.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns the following error code.

| Return Value/Code | Description |
| --- | --- |
| 0x00000032  ERROR\_NOT\_SUPPORTED | The request is not supported. This error value is returned when **DsrDeregisterDnsHostRecords** is called on a machine that is not a DC. |

The server SHOULD determine if the client has sufficient [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940) (as described in section [3.5.4.2](#Section_1ec948862b6445afb68e3d9faa36617c)) with the Access Request mask set to the NETLOGON\_CONTROL\_ACCESS mask.

If the client does not have sufficient privilege, the server MUST return ERROR\_ACCESS\_DENIED.

If the *DnsHostName* parameter is not null, the server MUST attempt to delete the DNS SRV records registered for the DC *DnsHostName*, as specified in [MS-ADTS] section 6.3.2.3.

If the *DomainGuid* parameter is not null, then the server MUST attempt to delete the domain-GUID-based SRV record.

If the *DsaGuid* parameter is not null, then the server MUST attempt to delete the domain CNAME record.

The deletion of [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba)-specific records MUST be attempted for every site in the enterprise of the DC on which the method is executed.

Unless stated otherwise, if the attempt to delete any records documented previously fails for any reason, then the server MUST ignore the error and continue message processing.

It is possible that this method call will create a time-consuming run that can generate significant network traffic for enterprises with many sites.

##### DsrUpdateReadOnlyServerDnsRecords (Opnum 48)

The DsrUpdateReadOnlyServerDnsRecords method SHOULD[<167>](#Appendix_A_167" \o "Product behavior note 167) allow an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to send a control command to a normal (writable) [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) for site-specific and CName types of [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) records update. For registration, site-specific records SHOULD be for the [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) in which RODC resides. For the types of DNS records, see [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.2.

1. NTSTATUS DsrUpdateReadOnlyServerDnsRecords(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in, unique, string] wchar\_t\* SiteName,
7. [in] ULONG DnsTtl,
8. [in, out] PNL\_DNS\_NAME\_INFO\_ARRAY DnsNames
9. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed) (as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)) that represents the connection to the normal (writable) DC.

**ComputerName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the client computer [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf).

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure (as specified in section 2.2.1.1.5) that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3) that will be used to authenticate the client.

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure that contains the server return authenticator.

**SiteName:** A pointer to a null-terminated Unicode string that contains the site name where the RODC resides.

**DnsTtl:** The Time To Live value, in seconds, for DNS records.

**DnsNames:** A pointer to an [NL\_DNS\_NAME\_INFO\_ARRAY (section 2.2.1.2.6)](#Section_8ae8a92eb63a43fd935097f1cab1c148) structure that contains an array of [NL\_DNS\_NAME\_INFO](#Section_1c7e652045a243e1ac0b43e771f85b14) structures.

**Return Values:** The method returns 0x00000000 (NO\_ERROR) on success; otherwise, it returns a nonzero error code.

On receiving this call, the server performs the following steps:

* Verifies that the server is a normal (writable) DC; otherwise, the server MUST return STATUS\_NOT\_SUPPORTED.[<168>](#Appendix_A_168" \o "Product behavior note 168)
* Verifies that the caller (ComputerName) is an RODC; otherwise, the server MUST return STATUS\_NOT\_SUPPORTED.
* Verifies that the *Authenticator* passed, and compute the *ReturnAuthenticator*, as specified in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806). If the *Authenticator* verification fails, the server MUST return STATUS\_ACCESS\_DENIED.
* Validates the requested DNS name type. Only site-specific and CName types are supported. For an unsupported DNS name type, sets the DNS name status to STATUS\_NOT\_SUPPORTED.
* Validates the site name for site-specific DNS name registration. Sets DNS name status to STATUS\_ACCESS\_DENIED for an invalid site name.
* Validates Ndnc [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) for the registration of NlDnsNdncDomainName DnsDomainInfoType. Sets DNS name status to STATUS\_ACCESS\_DENIED for an invalid Ndnc domain name.

This method can be called only by a machine that has established a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the server.

#### Secure Channel Establishment and Maintenance Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used to establish the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca), as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NetrServerReqChallenge (Opnum 4)

The NetrServerReqChallenge method SHOULD[<169>](#Appendix_A_169" \o "Product behavior note 169) receive a [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) and return a [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9) .

1. NTSTATUS NetrServerReqChallenge(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_CREDENTIAL ClientChallenge,
5. [out] PNETLOGON\_CREDENTIAL ServerChallenge
6. );

**PrimaryName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** A [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer calling this method.

**ClientChallenge:** A pointer to a [NETLOGON\_CREDENTIAL](#Section_d55e263271634f6cb6624b870e8cc1cd) structure, as specified in section 2.2.1.3.4, that contains the client challenge.

**ServerChallenge:** A pointer to a NETLOGON\_CREDENTIAL structure, as specified in section 2.2.1.3.4, that contains the server challenge response.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Apply Common Error Processing Rule B, specified in section 3, to the *PrimaryName* parameter.

The server MUST generate 64 bits of random data as the server challenge to be returned in the *ServerChallenge* parameter. The *ServerChallenge* is saved in the **ChallengeTable**, along with the client name passed in the *ComputerName* parameter and the client challenge passed in the *ClientChallenge* parameter.

##### NetrServerAuthenticate3 (Opnum 26)

The NetrServerAuthenticate3 method SHOULD[<170>](#Appendix_A_170" \o "Product behavior note 170) mutually authenticate the client and the server and establish the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to be used for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) message protection between the client and the server. It is called after the [NetrServerReqChallenge](#Section_5ad9db9f74414ce58c7b7b771e243d32) method, as specified in section 3.5.4.4.1.

1. NTSTATUS NetrServerAuthenticate3(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_CREDENTIAL ClientCredential,
7. [out] PNETLOGON\_CREDENTIAL ServerCredential,
8. [in, out] ULONG \* NegotiateFlags,
9. [out] ULONG \* AccountRid
10. );

**PrimaryName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that identifies the name of the account that contains the [**secret key**](#gt_dc4cd75d-71f9-4ceb-8938-504d0c6b2fbf) (password) that is shared between the client and the server, as described in section [1.5](#Section_41679899e81b41bfaddae269ce9dc33d).[<171>](#Appendix_A_171" \o "Product behavior note 171)

**SecureChannelType:** A [NETLOGON\_SECURE\_CHANNEL\_TYPE](#Section_4d1235e32c964e9fa1473cb338a0d09f) enumerated value, as specified in section 2.2.1.3.13, that indicates the type of the secure channel being established by this call.

**ComputerName:** A null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer calling this method.

**ClientCredential:** A pointer to a [NETLOGON\_CREDENTIAL](#Section_d55e263271634f6cb6624b870e8cc1cd) structure, as specified in section 2.2.1.3.4, that contains the supplied client [**credentials**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8), as specified in section [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585).

**ServerCredential:** A pointer to a NETLOGON\_CREDENTIAL structure, as specified in section 2.2.1.3.4, that contains the returned server credentials.

**NegotiateFlags:** A pointer to a 32-bit set of bit flags in little-endian format that indicate features supported. As input, the set of flags are those requested by the client and SHOULD be the same as [ClientCapabilities](#Section_fd1e918135a045d3b39cb7453dfc0af5). As output, they are the bit-wise AND of the client's requested capabilities and the server's [ServerCapabilities](#Section_b8d168acebb642f4bfb27a84377f2cbc). For more details, see section [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed).

**AccountRid:** A pointer that receives the [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the account specified by the *AccountName* parameter. ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.5.2.4 describes how this RID is assigned at account creation time.) This value is stored in the **AccountRid** ADM element within the ClientSessionInfo table.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Apply Common Error Processing Rule B, specified in section 3, to the *PrimaryName* parameter.

If the *AccountName* parameter is the name of a domain trust object, and there is a period at the end of the parameter name, the period is ignored during processing.

The server SHOULD[<172>](#Appendix_A_172" \o "Product behavior note 172) check the *SecureChannelType* parameter.

The server MUST compute the mask of supported Netlogon Options.

If **RejectDES** is set to TRUE and neither flag O nor flag W is specified by the client, the server MUST fail the session-key negotiation and return STATUS\_DOWNGRADE\_DETECTED.

If **RejectMD5Clients** is set to TRUE and flag W is not specified by the client, the server MUST fail the session-key negotiation and return STATUS\_DOWNGRADE\_DETECTED.

The server MUST set **ClientStoredCredential** to 0.

The server MUST set **ServerStoredCredential** to the value of the *ClientCredential* parameter.

The server MUST compute or retrieve the NTOWFv1 (as specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the client computer password and use it to compute a session key, as described in section [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63). If the server cannot compute or retrieve the NTOWFv1 of the client computer password, it MUST return STATUS\_NO\_TRUST\_SAM\_ACCOUNT.

The server MUST compute the client Netlogon credential as described in section 3.1.4.4, and compare the result with the client Netlogon credential passed from the client for verification. The computation is performed using the *ClientChallenge* from the **ChallengeTable**. If the comparison fails, session-key negotiation fails, and the server MUST return STATUS\_ACCESS\_DENIED.

The server MUST compute the server Netlogon credential to be returned to the client.

The server MUST obtain the RID to be returned in the *AccountRid* parameter by performing external behavior consistent with locally invoking **SamrLookupNamesInDomain** ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 3.1.5.11.2), using the following parameters:

* *DomainHandle* is set to the value received by performing external behavior consistent with locally invoking **SamrOpenDomain** ([MS-SAMR] section 3.1.5.1.5).
* *Count* is set to the value of 1.
* *Names* is set to an array with a length of 1, and is the only array element set to the value of <AccountName>.

If the call returns any error code other than STATUS\_SUCCESS, the server MUST return that error code.

The server MUST obtain the value of the DomainHandle parameter used when invoking **SamrLookupNamesInDomain** by performing external behavior consistent with locally invoking **SamrOpenDomain** ([MS-SAMR] section 3.1.5.1.5), using the following parameters:

* *ServerHandle* is set to the value returned by performing external behavior consistent with locally invoking **SamrConnect** ([MS-SAMR] section 3.1.5.1.4).
* *DesiredAccess* is set to the value DOMAIN\_LOOKUP.
* *DomainId* is set to the value of DomainSid (section 3.5.1).

If the call returns any error code other than STATUS\_SUCCESS, the server MUST return that error code.

The server MUST obtain the value of the *ServerHandle* parameter used when invoking **SamrOpenDomain** by performing external behavior consistent with locally invoking **SamrConnect** ([MS-SAMR] section 3.1.5.1.4), using the following parameters:

* *ServerName* is set to the value of the NetBIOS form of the server [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b).
* *DesiredAccess* is set to the value SAM\_SERVER\_LOOKUP\_DOMAIN.

If the call returns any error code other than STATUS\_SUCCESS, the server MUST return that error code.

##### NetrServerAuthenticate2 (Opnum 15)

The NetrServerAuthenticate2 method[<173>](#Appendix_A_173" \o "Product behavior note 173) is a predecessor to the [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) method, as specified in section 3.5.4.4.2. All parameters of this method have the same meanings as the identically named parameters of the NetrServerAuthenticate3 method.

1. NTSTATUS NetrServerAuthenticate2(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_CREDENTIAL ClientCredential,
7. [out] PNETLOGON\_CREDENTIAL ServerCredential,
8. [in, out] ULONG \* NegotiateFlags
9. );

Message processing is identical to NetrServerAuthenticate3, except for the following:

The *AccountRid* parameter is not present in NetrServerAuthenticate2.

##### NetrServerAuthenticate (Opnum 5)

The NetrServerAuthenticate method[<174>](#Appendix_A_174" \o "Product behavior note 174) is a predecessor to the [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) method (section 3.5.4.4.2). All parameters of this method have the same meanings as the identically named parameters of the NetrServerAuthenticate3 method.

1. NTSTATUS NetrServerAuthenticate(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_CREDENTIAL ClientCredential,
7. [out] PNETLOGON\_CREDENTIAL ServerCredential
8. );

Message processing is identical to NetrServerAuthenticate3, as specified in section 3.5.4.4.2, except for the following:

* The *NegotiateFlags* parameter is not present in NetrServerAuthenticate. Message processing would be identical to an invocation of NetrServerAuthenticate3 with the *NegotiateFlags* parameter set to 0.
* The *AccountRid* parameter is not present in NetrServerAuthenticate.

##### NetrServerPasswordSet2 (Opnum 30)

The NetrServerPasswordSet2 method SHOULD[<175>](#Appendix_A_175" \o "Product behavior note 175) allow the client to set a new clear text password for an account used by the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) (as specified in section [1.5](#Section_41679899e81b41bfaddae269ce9dc33d)) for setting up the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) from the client. A [**domain member**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65) uses this function to periodically change its machine account password. A [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) uses this function to periodically change the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password for all directly trusted [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).[<176>](#Appendix_A_176" \o "Product behavior note 176)

1. NTSTATUS NetrServerPasswordSet2(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
7. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
8. [in] PNL\_TRUST\_PASSWORD ClearNewPassword
9. );

**PrimaryName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the account whose password is being changed.[<177>](#Appendix_A_177" \o "Product behavior note 177)

**SecureChannelType:** An enumerated value that describes the secure channel to be used for authentication, as specified in section [2.2.1.3.13](#Section_4d1235e32c964e9fa1473cb338a0d09f).

**ComputerName:** The null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the computer making the request.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the encrypted logon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) and a time stamp.

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ClearNewPassword:** A pointer to an [NL\_TRUST\_PASSWORD](#Section_52d5bd865caf47aaaae4cadf7339ec83) structure, as specified in section 2.2.1.3.7, that contains the new password encrypted as specified in [Calling NetrServerPasswordSet2 (section 3.4.5.2.5)](#Section_b348c16e5cdb4414876de8b0e12fbae0).

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the secure channel to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Apply Common Error Processing Rule B, specified in section 3, to the *PrimaryName* parameter.

If the server *RefusePasswordChange* variable (section [3.5.1](#Section_b8d168acebb642f4bfb27a84377f2cbc)) is set and the *SecureChannelType* is WorkstationSecureChannel, the server MUST return STATUS\_WRONG\_PASSWORD.

The server MUST decrypt the new password supplied in the *ClearNewPassword* parameter, by using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the **NegotiateFlags** member of the **ClientSessionInfo** table entry for *ComputerName*) and the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) established as the [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) key. The NTOWFv1 (as specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the cleartext password MUST be computed.

The server MUST compute or retrieve (see unicodePwd, [[MS-ADA3]](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0) section 2.332) the NTOWFv1 of the current client machine password, which is stored as the result of the [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) on the clear text password for the AccountName. If the current password matches the new password, success is returned to the client, but no actual password change is performed.

The server MUST change the SharedSecret abstract value to the new password supplied in the *ClearNewPassword* parameter. If the value of the **PasswordVersionPresent** field of the ClearNewPassword.Buffer parameter is equal to 0x02231968, the server MUST change the **TrustPasswordVersion** abstract value to the value of the **PasswordVersionNumber** field of the ClearNewPassword.Buffer parameter. See section [2.2.1.3.8](#Section_cba0e87eb91f411b9be86fd321e126b7) for more details about the type of the *ClearNewPassword* parameter.

This method can only be called by a machine that has established a secure channel with the server.

This method also returns errors based on Common Error Processing Rule D, specified in section 3.

##### NetrServerPasswordSet (Opnum 6)

The NetrServerPasswordSet method SHOULD[<178>](#Appendix_A_178" \o "Product behavior note 178) set a new [**one-way function (OWF)**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of a password for an account used by the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) (as described in section [1.5](#Section_41679899e81b41bfaddae269ce9dc33d)) for setting up the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) from the client.

1. NTSTATUS NetrServerPasswordSet(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
7. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
8. [in] PENCRYPTED\_NT\_OWF\_PASSWORD UasNewPassword
9. );

**PrimaryName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the account whose password is being changed.[<179>](#Appendix_A_179" \o "Product behavior note 179)

**SecureChannelType:** An enumerated value (specified in section [2.2.1.3.13](#Section_4d1235e32c964e9fa1473cb338a0d09f)) that indicates the type of secure channel used by the client.

**ComputerName:** A null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer calling this method.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**UasNewPassword:** A pointer to an ENCRYPTED\_NT\_OWF\_PASSWORD structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.3.3 and encrypted by the algorithm specified in section [3.4.5.2.6](#Section_0be5436ec68c46478ecafe0be3512b9b).

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the secure channel to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

If the *RefusePasswordChange* variable (section [3.5.1](#Section_b8d168acebb642f4bfb27a84377f2cbc)) is set and the *SecureChannelType* is WorkstationSecureChannel, the server MUST return STATUS\_WRONG\_PASSWORD.

The server MUST decrypt the new password that is supplied in the *UasNewPassword* parameter by using the inverse to the encryption algorithm that is specified in [MS-SAMR] section 2.2.11.1.1, Encrypt an NT Hash or LM Hash Value with a specified key. The [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is the specified key input, and the [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) keys are derived using the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4.

The server MUST compute or retrieve the NTOWFv1 (as specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the current client machine password, which is stored as an OWF of the clear-text password for the account.

The server MUST compute or retrieve the NTOWFv1 of the old client machine password and compare it to the NTOWFv1 of the new password supplied in the *UasNewPassword* parameter; if they match, the server MUST return STATUS\_ACCESS\_DENIED.

This method can only be called by a machine that has established a secure channel with the server.

This method also returns errors based on Common Error Processing Rule D, specified in section 3.

##### NetrServerPasswordGet (Opnum 31)

The NetrServerPasswordGet method SHOULD[<180>](#Appendix_A_180" \o "Product behavior note 180) allow a BDC to get a machine account password from the [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) with the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) role in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. NTSTATUS NetrServerPasswordGet(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE AccountType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
7. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
8. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNtOwfPassword
9. );

**PrimaryName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the account to retrieve the password for.[<181>](#Appendix_A_181" \o "Product behavior note 181)

**AccountType:** A [NETLOGON\_SECURE\_CHANNEL\_TYPE](#Section_4d1235e32c964e9fa1473cb338a0d09f) enumerated value, as specified in section 2.2.1.3.13, that describes the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to be used for authentication.

**ComputerName:** A null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the DC making the call.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the encrypted logon [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) and a time stamp.

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**EncryptedNtOwfPassword:** A pointer to an [ENCRYPTED\_NT\_OWF\_PASSWORD](#Section_f7458576d53847cdb387b6f98449a0ee) structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.3.3, that contains the [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) password of the account.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Verify that the caller of this method is not an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) or PDC; otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Verify that AccountName is not NULL and AccountType flags are valid; otherwise, the server MUST return STATUS\_INVALID\_PARAMETER.
* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Apply Common Error Processing Rule B, specified in section 3, to the *PrimaryName* parameter.
* The server uses the server name passed in the PrimaryName parameter to look up the domain that the server hosts. If the name is not found, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME.
* Using the *ComputerName* for the secure channel to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

The server MUST retrieve the current OWF of the password for the account identified by the *AccountName* and *AccountType* parameters. If the *AccountType* is TrustedDnsDomainSecureChannel or TrustedDomainSecureChannel, then the SharedSecret of the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) will be used. All other types of **SecureChannelType** that can be used require that the SharedSecret of the computer account is used.

The server MUST retrieve the current OWF of the client password and encrypt it with the key that is derived by using the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) as the specified 16-byte key. The specified 16-byte key uses the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4. The encrypted version of the password MUST be returned in the *EncryptedNtOwfPassword* parameter.

This method can only be called by a machine that has established a secure channel with the server.

##### NetrServerTrustPasswordsGet (Opnum 42)

The NetrServerTrustPasswordsGet method SHOULD[<182>](#Appendix_A_182" \o "Product behavior note 182) return the encrypted current and previous passwords for an account in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). This method is called by a client to retrieve the current and previous account passwords from a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd). The account name requested MUST be the name used when the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) was created, unless the method is called on a [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) by a DC, in which case it can be any valid account name.

1. NTSTATUS NetrServerTrustPasswordsGet(
2. [in, unique, string] LOGONSRV\_HANDLE TrustedDcName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
7. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
8. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNewOwfPassword,
9. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedOldOwfPassword
10. );

**TrustedDcName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the client account in the domain for which the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) password MUST be returned.[<183>](#Appendix_A_183" \o "Product behavior note 183)

**SecureChannelType:** A [NETLOGON\_SECURE\_CHANNEL\_TYPE](#Section_4d1235e32c964e9fa1473cb338a0d09f) enumerated value, as specified in section 2.2.1.3.13, that indicates the type of the secure channel being established by this call.

**ComputerName:** The null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**EncryptedNewOwfPassword:** A pointer to an [ENCRYPTED\_NT\_OWF\_PASSWORD](#Section_f7458576d53847cdb387b6f98449a0ee) structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.3.3, that contains the NTOWFv1 (as specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the current password, encrypted as specified in [MS-SAMR] section 2.2.11.1.1, Encrypting an NT Hash or LM Hash Value with a specified key. The [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is the specified 16-byte key that is used to derive the password's keys. The specified 16-byte key uses the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4.

**EncryptedOldOwfPassword:** A pointer to an ENCRYPTED\_NT\_OWF\_PASSWORD structure, as specified in [MS-SAMR] section 2.2.3.3, that contains the NTOWFv1 (as specified in NTLM v1 Authentication in [MS-NLMP] section 3.3.1) of the previous password, encrypted as specified in [MS-SAMR] section 2.2.11.1.1, Encrypting an NT Hash or LM Hash Value with a specified key. The session key is the specified 16-byte key that is used to derive the password's keys. The specified 16-byte key uses the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

Message processing is identical to [NetrServerGetTrustInfo](#Section_4c2296c3c6f047fc9f01a6fe17bf1d5b), as specified in section 3.5.4.7.6, except for the following:

* The *TrustInfo* parameter is not present in NetrServerTrustPasswordsGet.

##### NetrLogonGetDomainInfo (Opnum 29)

The NetrLogonGetDomainInfo method SHOULD[<184>](#Appendix_A_184" \o "Product behavior note 184) return information that describes the current [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) to which the specified client belongs.

1. NTSTATUS NetrLogonGetDomainInfo(
2. [in, string] LOGONSRV\_HANDLE ServerName,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD Level,
7. [in, switch\_is(Level)] PNETLOGON\_WORKSTATION\_INFORMATION WkstaBuffer,
8. [out, switch\_is(Level)] PNETLOGON\_DOMAIN\_INFORMATION DomBuffer
9. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the client computer issuing the request.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**Level:** The information level requested by the client. The *DomBuffer* parameter contains one of the following structures, based on the value of this field.

| Value | Meaning |
| --- | --- |
| 0x00000001 | The *DomBuffer* contains a [NETLOGON\_DOMAIN\_INFO](#Section_440c3430ed5f481db60274db422df3c8) structure. |
| 0x00000002 | The *DomBuffer* contains a [NETLOGON\_LSA\_POLICY\_INFO](#Section_4676ac8320994e33b680502fd8a32dbd) structure. |

**WkstaBuffer:** A pointer to a [NETLOGON\_WORKSTATION\_INFORMATION](#Section_7520d43a751d4d52928244bb48fcc6d4) structure, as specified in section 2.2.1.3.9, that contains information about the client workstation.

**DomBuffer:** A pointer to a [NETLOGON\_DOMAIN\_INFORMATION](#Section_3077715970ef498290a1f8e93aaeb985) structure, as specified in section 2.2.1.3.12, that contains information about the domain or policy information.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Verify that the *WkstaBuffer* parameter is not NULL. If it is, the server SHOULD return STATUS\_INVALID\_PARAMETER.[<185>](#Appendix_A_185" \o "Product behavior note 185)
* Verify that the *Level* parameter is set to 1 or 2. All other values are invalid, and STATUS\_INVALID\_LEVEL MUST be returned.
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

If the *Level* parameter is set to 1, the return structure pointed to by *DomBuffer* MUST be generated as follows:

* NETLOGON\_DOMAIN\_INFO.PrimaryDomain.DomainName MUST be set to **NetbiosDomainName**.
* NETLOGON\_DOMAIN\_INFO.PrimaryDomain.DnsDomainName MUST be set to **DnsDomainName**.
* NETLOGON\_DOMAIN\_INFO.PrimaryDomain.DnsForestName MUST be set to **DnsForestName**.
* NETLOGON\_DOMAIN\_INFO.PrimaryDomain.DomainGuid MUST be set to **DomainGuid**.
* NETLOGON\_DOMAIN\_INFO.PrimaryDomain.DomainSid MUST be set to **DomainSid**.
* NETLOGON\_DOMAIN\_INFO.WorkstationFlags MUST be set with the bitwise AND of NETLOGON\_WORKSTATION\_INFORMATION.WorkstationInfo.WorkstationFlags and 0x3.
* NETLOGON\_DOMAIN\_INFO.TrustedDomainCount MUST be set to the number of elements of the [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain list returned by performing the external behavior consistent with locally invoking LsarEnumerateTrustedDomainsEx ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.7). The *EnumerationContext* parameter MUST be set to 0 and *PreferredMaximumLength* SHOULD[<186>](#Appendix_A_186" \o "Product behavior note 186) be set to 4096. A policy handle is not needed locally.
* NETLOGON\_DOMAIN\_INFO.TrustedDomains MUST be set to a TrustedDomainCount-sized array of NETLOGON\_ONE\_DOMAIN\_INFO structures. Each structure MUST be generated as follows:
  + NETLOGON\_ONE\_DOMAIN\_INFO.DomainName MUST be set to the NetBIOS [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) of the trusted domain.
  + NETLOGON\_ONE\_DOMAIN\_INFO.DnsDomainName MUST be set to the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) domain name of the trusted domain.
  + NETLOGON\_ONE\_DOMAIN\_INFO.DnsForestName MUST be set to NULL string.
  + NETLOGON\_ONE\_DOMAIN\_INFO.DomainGuid MUST be set to the domain [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1) of the trusted domain.
  + NETLOGON\_ONE\_DOMAIN\_INFO.DomainSid SHOULD[<187>](#Appendix_A_187" \o "Product behavior note 187) be set to the domain [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) of the trusted domain.
* NETLOGON\_DOMAIN\_INFO.SupportedEncTypes MUST be set to the value of the msDS-SupportedEncryptionTypes attribute ([[MS-ADA2]](%5bMS-ADA2%5d.pdf#Section_e20ebc4e528540bab3bdffcb81c2783e) section 2.464) of the *ComputerName* account. If the msDS-SupportedEncryptionTypes attribute does not exist, then set NETLOGON\_DOMAIN\_INFO.SupportedEncTypes to 0xFFFFFFFF.

| Structure | Reference |
| --- | --- |
| NETLOGON\_DOMAIN\_INFO | For details, see section 2.2.1.3.11. |
| NETLOGON\_WORKSTATION\_INFO | For details, see section [2.2.1.3.6](#Section_3ae9e9a9a3034fa58e11823d9e7e1e61). |
| DS\_DOMAIN\_TRUSTSW | For details, see section [2.2.1.6.2](#Section_7de9866ed3ef4a9f98a5c2dcff1e61c1). |
| NETLOGON\_ONE\_DOMAIN\_INFO | For details, see section [2.2.1.3.10](#Section_77cd977686124dab9748bfb07247fd4c). |

If the Level parameter is set to 2:

* NETLOGON\_DOMAIN\_INFO.LsaPolicy.LsaPolicySize MUST be set to 0.
* NETLOGON\_DOMAIN\_INFO.LsaPolicy.LsaPolicy MUST be set to NULL.

If the WkstaBuffer.*WorkstationInfo* pointer is NULL, no further processing occurs and NERR\_Success MUST be returned.

If WkstaBuffer.*WorkstationInfo*.*WorkstationFlags* has the 0x2 bit set, NETLOGON\_DOMAIN\_INFO.DnsHostNameInDs is set to the **dNSHostName** attribute ([[MS-ADA1]](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f) section 2.185) of the client account. The **dNSHostName** attribute is validated against the constraints specified in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.5.3.1.1.2. If there was a change in domain naming, this value holds the previous DNS host name because the AD query is done prior to changing the value. If WkstaBuffer.*WorkstationInfo*.*WorkstationFlags* does not have the 0x2 bit set, the server adds the following [**SPNs**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4) to the **ServicePrincipalName** attribute of the clients account:

* HOST/<Netbios name>
* HOST/<FQDN name>

WkstaBuffer.*WorkstationInfo*.*OsName* and WkstaBuffer.*WorkstationInfo*.*OsVersion* SHOULD be processed as specified in section 2.2.1.3.6. If WkstaBuffer.*WorkstationInfo*.*OsName* and WkstaBuffer.*WorkstationInfo*.*OsVersion* are not specified, then use a generic string, for example, "Windows unknown version" to update the operatingSystem attribute. If WkstaBuffer.*WorkstationInfo*.*OsVersion* is specified but WkstaBuffer.*WorkstationInfo*.*OsName* is not, then a different generic string SHOULD[<188>](#Appendix_A_188" \o "Product behavior note 188) be used to update the **operatingSystem** attribute, depending on the value of WkstaBuffer.*WorkstationInfo*.*OsVersion*.*wProductType*.[<189>](#Appendix_A_189" \o "Product behavior note 189)

If WkstaBuffer*.WorkstationInfo.KerberosSupportedEncryptionTypes* is set, NETLOGON\_DOMAIN\_INFO.SupportedEncTypes is set to the **msDS-SupportedEncryptionTypes** attribute ([MS-ADA2] section 2.464) of the client account.

This method can only be called by a machine that has established a secure channel with the server.

##### NetrLogonGetCapabilities (Opnum 21)

The NetrLogonGetCapabilities method is used by clients to confirm the server capabilities after a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) has been established.[<190>](#Appendix_A_190" \o "Product behavior note 190)

1. NTSTATUS NetrLogonGetCapabilities(
2. [in, string] LOGONSRV\_HANDLE ServerName,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD QueryLevel,
7. [out, switch\_is(QueryLevel)] PNETLOGON\_CAPABILITIES ServerCapabilities
8. );

**ServerName:** A [LOGONSRV\_HANDLE](#Section_3b224201b53143e28c79b61f6dea8640) [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string handle of the server that is handling the request.

**ComputerName:** A string that contains the name of the computer.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure that contains the server return authenticator.

**QueryLevel:** Specifies the level of information to return from the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) being queried. A value of 0x00000001 causes return of a [NETLOGON\_CAPABILITIES](#Section_f03cad67077f404280b0cdc38dca9968) structure that contains server capabilities.

**ServerCapabilities:** A pointer to a 32-bit set of bit flags that identify the server's capabilities.[<191>](#Appendix_A_191" \o "Product behavior note 191)

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

Upon receiving this call, the server MUST perform the following validation steps:[<192>](#Appendix_A_192" \o "Product behavior note 192)

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Verify that the *QueryLevel* parameter is set to 1. All other values are invalid, and STATUS\_INVALID\_LEVEL MUST be returned.
* Using the ComputerName for the secure channel to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

If *ServerCapabilities* bit W is true, then *ServerCapabilities* MUST be set to the ServerSessionInfo.NegotiateFlags being used by the secure channel of the calling client. Otherwise, the server MUST return STATUS\_NOT\_IMPLEMENTED.

##### NetrChainSetClientAttributes (Opnum 49)

When an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) receives either the [NetrServerAuthenticate3](#Section_3a9ed16f801445ae80afc0ecb06e2db9) method or the [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) method with updates requested, it SHOULD[<193>](#Appendix_A_193" \o "Product behavior note 193) invoke the NetrChainSetClientAttributes method on a normal (writable) [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) to update to a client's computer account object in [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90).

1. NTSTATUS NetrChainSetClientAttributes(
2. [in, string, ref] LOGONSRV\_HANDLE PrimaryName,
3. [in, string, ref] wchar\_t\* ChainedFromServerName,
4. [in, string, ref] wchar\_t\* ChainedForClientName,
5. [in, ref] PNETLOGON\_AUTHENTICATOR Authenticator,
6. [in, out, ref] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
7. [in] DWORD dwInVersion,
8. [in, ref] [switch\_is(dwInVersion)]
9. NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\* pmsgIn,
10. [in, out, ref] DWORD\* pdwOutVersion,
11. [in, out, ref] [switch\_is(\*pdwOutVersion)]
12. NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\* pmsgOut
13. );

**PrimaryName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ChainedFromServerName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the read-only DC that issues the request.

**ChainedForClientName:** The null-terminated Unicode string that contains the name of the client computer that called NetrServerAuthenticate3 or NetrLogonGetDomainInfo on the RODC.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure that contains the server return authenticator.

**dwInVersion:** One of the [NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES](#Section_548d751953d1489192d5f7d240c73496) union types selected based on the value of the *pmsgIn* field. The value MUST be 1.

**pmsgIn:** A pointer to an [NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1](#Section_f4ed8790d7e84ca18062d25784ed79e3) structure that contains the values to update on the client's computer account object in Active Directory on the normal (writable) DC.

**pdwOutVersion:** A pointer to one of the [NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES](#Section_b8491488cbb6452bbab1b0f4390bca59) union types selected based on the value of the *pmsgIn* field. The value MUST be 1.

**pmsgOut:** A pointer to an [NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1](#Section_ab43a76224e245c387011838589d80fe) structure that contains information on the client workstation and the [**writable domain controller**](#gt_9d964ddb-09d6-4a1b-b27b-42adabc07993). For how it is populated by the server, see below.

**Return Values:** The method returns 0x00000000 on success.

On receiving this call, the normal (writable) DC MUST perform the following validation steps.

* Verify that the server is a normal (writable) DC machine; otherwise, the server MUST return STATUS\_NOT\_SUPPORTED.
* Verify that the *dwInVersion* parameter is set to 1. All other values are invalid and STATUS\_NOT\_SUPPORTED MUST be returned.
* Verify that the *pdwOutVersion* parameter is set to 1. All other values are invalid and STATUS\_NOT\_SUPPORTED MUST be returned.
* Verify that the *Authenticator* passed, and compute the *ReturnAuthenticator*, as specified in section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806). If the *Authenticator* verification fails, the server MUST return STATUS\_ACCESS\_DENIED.[<194>](#Appendix_A_194" \o "Product behavior note 194)

The return structure MUST be generated as follows:

* NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES.HubName MUST be set to the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the writable domain controller.
* If NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES.OldDnsHostName is not NULL, it MUST be set to the client's [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) host name, if any. If there was a change in [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) naming, this value holds the previous DNS host name.
* If NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES.SupportedEncTypes is not NULL, it MUST be set to the supported encryption algorithms.

#### Pass-Through Authentication Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used for generic pass-though, user logon, and user logoff as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NetrLogonSamLogonEx (Opnum 39)

The NetrLogonSamLogonEx method SHOULD[<195>](#Appendix_A_195" \o "Product behavior note 195) provide an extension to [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a) that accepts an extra flags parameter and uses Secure [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) ([[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) section 3.3.1.5.2) instead of Netlogon [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3). This method handles logon requests for the [**SAM**](#gt_0b53d5bb-74ab-4705-8657-c22d32781103) accounts and allows for generic pass-through authentication, as specified in section [3.2.4.1](#Section_fe2775d4a3e24971a2558eef8dd27a27). For more information about fields and structures used by Netlogon pass-through methods, see section [1.3.8.1.3](#Section_115abd4a7a1947a3af0ebdc9631a36d1).

1. NTSTATUS NetrLogonSamLogonEx(
2. [in] handle\_t ContextHandle,
3. [in, unique, string] wchar\_t\* LogonServer,
4. [in, unique, string] wchar\_t\* ComputerName,
5. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
6. [in, switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
7. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
8. [out, switch\_is(ValidationLevel)]
9. PNETLOGON\_VALIDATION ValidationInformation,
10. [out] UCHAR \* Authoritative,
11. [in, out] ULONG \* ExtraFlags
12. );

**ContextHandle:** A primitive RPC handle that identifies a particular client/server binding, as specified in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**LogonServer:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the server that will handle the logon request.

**ComputerName:** The null-terminated Unicode string that contains the NetBIOS name of the client computer sending the logon request.

**LogonLevel:** A [NETLOGON\_LOGON\_INFO\_CLASS](#Section_8c7808e54e5c420e9c9047286da2218f) enumerated type, as specified in section 2.2.1.4.16, that specifies the type of the logon information passed in the *LogonInformation* parameter.

**LogonInformation:** A pointer to a [NETLOGON\_LEVEL](#Section_d0128545f74b4d89afd942621dff24c4) structure, as specified in section 2.2.1.4.6, that describes the logon request information.

**ValidationLevel:** A [NETLOGON\_VALIDATION\_INFO\_CLASS](#Section_95154ae4d30543e582e4d5353e0f117c) enumerated type, as specified in section 2.2.1.4.17, that contains the validation level requested by the client.

**ValidationInformation:** A pointer to a [NETLOGON\_VALIDATION](#Section_5eb0b7cb3a55477b92fcc236bd5873fa) structure, as specified in section 2.2.1.4.14, that describes the user validation information returned to the client. The type of the NETLOGON\_VALIDATION used is determined by the value of the *ValidationLevel* parameter.

**Authoritative:** A pointer to a char value that represents a Boolean condition. FALSE is indicated by the value 0x00, and TRUE SHOULD[<196>](#Appendix_A_196" \o "Product behavior note 196) be indicated by the value 0x01 and MAY also be indicated by any nonzero value.

This Boolean value indicates whether the validation information is final. This field is necessary because the request might be forwarded through multiple servers. The value TRUE indicates that the validation information is an [**authoritative response**](#gt_1ed0d067-3bfd-4fd5-a68a-5e947d379858) and MUST remain unchanged. The value FALSE SHOULD indicate that the validation information is not an authoritative response and that the client can resend the request to another server.

**ExtraFlags:** A pointer to a set of bit flags that specify delivery settings. A flag is TRUE (or set) if its value is equal to 1. Output flags MUST be the same as input. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | D | C | B | A |

Where the bits SHOULD[<197>](#Appendix_A_197" \o "Product behavior note 197) be defined as:

| Value | Description |
| --- | --- |
| A | Request MUST be passed to the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) at the root of the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). |
| B | Request MUST be passed to the DC at the end of the first hop over a cross-[**forest trust**](#gt_035d9ce5-f117-4251-8d4d-127c462ec4a0). |
| C | Request was passed by an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to a DC in a different [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). |
| D | Request is an NTLM authentication package request passed by an RODC. |

All other bits MUST be set to zero and MUST be ignored on receipt. Flags A, B, C, and D can be combined and the server SHOULD honor the flags. Flags A and B require the server to take action to deliver the request, while flags C and D are informational and implementation-specific.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* The pointer contained in the *LogonInformation* parameter MUST NOT be NULL; otherwise, the server MUST return STATUS\_INVALID\_PARAMETER.
* Verify that the caller is using Secure RPC ([MS-RPCE] section 3.3.1.5.2); otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Verify that if bit B in *ExtraFlags* is enabled, then the domain's TAFT bit in the **trustAttributes** structure ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.6.7.9) is also enabled; otherwise, the server MUST return STATUS\_NO\_SUCH\_USER.
* Apply Common Error Processing Rule B, specified in section 3, to the *LogonServer* parameter.
* If the *LogonServer* parameter is not NULL, it is compared against the server's [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b). If the *LogonServer* parameter does not match the server's computer name or is NULL, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME. If the *LogonServer* parameter matches the server's computer name, processing proceeds.

If the server cannot service the request due to an implementation-specific condition, the server SHOULD return STATUS\_ACCESS\_DENIED.

The server uses the server name passed in the *LogonServer* parameter to look up the domain that the server hosts. If the name is not found, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME.

The server MUST decrypt data protected in transport:

* If the *LogonLevel* is **NetlogonInteractiveInformation** or **NetlogonInteractiveTransitiveInformation**, decrypt[<198>](#Appendix_A_198" \o "Product behavior note 198) the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_INTERACTIVE\_INFO (section 2.2.1.4.3)](#Section_af76351fef6946bca451e4c4b99bac4a) structure.
* If the *LogonLevel* is **NetlogonServiceInformation** or **NetlogonServiceTransitiveInformation**, decrypt[<199>](#Appendix_A_199" \o "Product behavior note 199) the **LmOwfPassword** and **NtOwfPassword** members in the [NETLOGON\_SERVICE\_INFO (section 2.2.1.4.4)](#Section_1c9f2af2e16445489428eae68a03537e) structure.
* If the *LogonLevel* is **NetlogonGenericInformation**, decrypt[<200>](#Appendix_A_200" \o "Product behavior note 200) the **LogonData** member in the [NETLOGON\_GENERIC\_INFO (section 2.2.1.4.2)](#Section_c03d6d959b5e43299645eedcdd167f6e) structure.

When the *LogonLevel* parameter is set to 4 (**NetlogonGenericInformation**), the call is for generic pass-through to authentication packages, and the *ValidationLevel* parameter MUST be 5 (**NetlogonValidationGenericInfo2**) or 4 (**NetlogonValidationGenericInfo**). If this is not true, the server MUST return STATUS\_INVALID\_INFO\_CLASS.[<201>](#Appendix_A_201" \o "Product behavior note 201)

If *LogonLevel* is not set to 4 (**NetlogonGenericInformation**), the ValidationLevel parameter MUST be 6 (**NetlogonValidationSamInfo4**) or 3 (**NetlogonValidationSamInfo2**) or 2 (**NetlogonValidationSamInfo**). If this is not true, the server MUST return STATUS\_INVALID\_INFO\_CLASS.[<202>](#Appendix_A_202" \o "Product behavior note 202) The data is opaque to Netlogon, and the parameters MUST be passed to NTLM ([[MS-APDS]](%5bMS-APDS%5d.pdf#Section_dd444344fd7e430eb3137e95ab9c338e) section 3.1).

If the request is not for the domain of which the server is a member and the server is a DC, then the server MUST perform external behavior consistent with locally invoking **LsarQueryTrustedDomainInfoByName** ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.5), using the following parameters (policy handle is not needed locally):

* *Domain* is set to the value of the *TrustedDomainName* parameter.
* *InformationClass* is set to the value of *TrustedDomainInformationEx*.

The server MUST also verify that:

* The **securityIdentifier** (Sid) field ([MS-ADTS] section 6.1.6.7.8) is not NULL,
* The **trustType** field ([MS-ADTS] section 6.1.6.7.15) is 1 or 2, and
* The **trustAttributes** field ([MS-ADTS] section 6.1.6.7.9) does not contain TRUST\_ATTRIBUTE\_UPLEVEL\_ONLY

If **LsarQueryTrustedDomainInfoByName** succeeds and returns the domain information in *TrustedDomainInformation*, the server MUST check if it has established a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the domain. If there is not an established secure channel then the server MUST return the error code STATUS\_NO\_SUCH\_USER. If there is an established secure channel then the server MUST call NetrLogonSamLogonEx using **LogonLevel**, **LogonInformation**, **ValidationLevel**, **ValidationInformation**, and **ExtraFlags** (**ExtraFlags** can be updated by the server before passing it to NetrLogonSamLogonEx on the DC) to the DC with which it has an established secure channel.

If an error is returned from an authentication package (in the case of generic pass-through) or from NTLM (in the case of logon), the error code MUST be propagated to the caller of this method.

If the *LogonLevel* is **NetlogonNetworkInformation** or **NetlogonNetworkTransitiveInformation**, the server MUST encrypt the *UserSessionKey* and the first two elements of the **ExpansionRoom** array in the [NETLOGON\_VALIDATION\_SAM\_INFO (section 2.2.1.4.11)](#Section_142a277fe16145ac8b95b94bb169b5da) or in the [NETLOGON\_VALIDATION\_SAM\_INFO2 (section 2.2.1.4.12)](#Section_2a12e28979044ecb9d836732200230c0) structure.

This method can be called only by a machine that has established a secure channel with the server.

This is the only NetrLogonSamLogon family method that uses secure channel and does not use Netlogon authenticator parameters.

##### NetrLogonSamLogonWithFlags (Opnum 45)

The NetrLogonSamLogonWithFlags method SHOULD[<203>](#Appendix_A_203" \o "Product behavior note 203) handle logon requests for the SAM accounts.

1. NTSTATUS NetrLogonSamLogonWithFlags(
2. [in, unique, string] LOGONSRV\_HANDLE LogonServer,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in, unique] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out, unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
7. [in, switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
8. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
9. [out, switch\_is(ValidationLevel)]
10. PNETLOGON\_VALIDATION ValidationInformation,
11. [out] UCHAR \* Authoritative,
12. [in, out] ULONG \* ExtraFlags
13. );

**LogonServer:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer calling this method.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**LogonLevel:** A [NETLOGON\_LOGON\_INFO\_CLASS](#Section_8c7808e54e5c420e9c9047286da2218f) structure, as specified in section 2.2.1.4.16, that specifies the type of logon information passed in the *LogonInformation* parameter.

**LogonInformation:** A pointer to a [NETLOGON\_LEVEL](#Section_d0128545f74b4d89afd942621dff24c4) structure, as specified in section 2.2.1.4.6, that describes the logon request information.

**ValidationLevel:** A [NETLOGON\_VALIDATION\_INFO\_CLASS](#Section_95154ae4d30543e582e4d5353e0f117c) enumerated type, as specified in section 2.2.1.4.17, that contains the validation level requested by the client.

**ValidationInformation:** A pointer to a [NETLOGON\_VALIDATION](#Section_5eb0b7cb3a55477b92fcc236bd5873fa) structure, as specified in section 2.2.1.4.14, that describes the user validation information returned to the client. The type of the NETLOGON\_VALIDATION used is determined by the value of the *ValidationLevel* parameter.

**Authoritative:** A pointer to a char value representing a Boolean condition. FALSE is indicated by the value 0x00; TRUE SHOULD[<204>](#Appendix_A_204" \o "Product behavior note 204) be indicated by the value 0x01 and MAY also be indicated by any nonzero value.

This Boolean value indicates whether the validation information is an [**authoritative response**](#gt_1ed0d067-3bfd-4fd5-a68a-5e947d379858). This field is necessary because the request might be forwarded through multiple servers. A value of TRUE indicates that the validation information is final and MUST remain unchanged. The value FALSE SHOULD indicate that the validation information is not an authoritative response and that the client can resend the request to another server.

**ExtraFlags:** A pointer to a set of bit flags that specify delivery settings. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | D | C | B | A |

Where the bits SHOULD[<205>](#Appendix_A_205" \o "Product behavior note 205) defined as:

| Value | Description |
| --- | --- |
| A | Request is passed to the [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) at the root of the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). |
| B | Request is passed to the DC at the end of the first hop over a cross-[**forest trust**](#gt_035d9ce5-f117-4251-8d4d-127c462ec4a0). |
| C | Request is passed by an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to a DC in a different [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). |
| D | Request is an NTLM authentication package request passed by an RODC. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

Message processing is identical to [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a), as specified in section 3.5.4.5.3, except for the following:

* NetrLogonSamLogonWithFlags contains an additional parameter named *ExtraFlags*.

##### NetrLogonSamLogon (Opnum 2)

The NetrLogonSamLogon method[<206>](#Appendix_A_206" \o "Product behavior note 206) is a predecessor to the [NetrLogonSamLogonWithFlags](#Section_d17f1077de4b4fcd886739068cb789f5) method (section 3.5.4.5.2). All parameters of this method have the same meanings as the identically named parameters of the NetrLogonSamLogonWithFlags method.

1. NTSTATUS NetrLogonSamLogon(
2. [in, unique, string] LOGONSRV\_HANDLE LogonServer,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in, unique] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out, unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
7. [in, switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
8. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
9. [out, switch\_is(ValidationLevel)]
10. PNETLOGON\_VALIDATION ValidationInformation,
11. [out] UCHAR \* Authoritative
12. );

Message processing is identical to [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd), as specified in section 3.5.4.5.1, except for the following:

* The method uses Netlogon [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3), so instead of checking for Secure [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331), the server MUST confirm the validity of the *Authenticator* (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)) that it received using the ComputerName for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table. If the *Authenticator* parameter is valid, the server MUST compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* The ExtraFlags parameter is not processed.

This method can only be called by a machine that has established a secure channel with the server.

On receiving this call, the server MUST perform the following validation step:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).

##### NetrLogonSamLogoff (Opnum 3)

The NetrLogonSamLogoff method SHOULD[<207>](#Appendix_A_207" \o "Product behavior note 207) update the user **lastLogoff** attribute for the SAM accounts.

1. NTSTATUS NetrLogonSamLogoff(
2. [in, unique, string] LOGONSRV\_HANDLE LogonServer,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in, unique] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out, unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
7. [in, switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation
8. );

**LogonServer:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** The [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer calling this method.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**LogonLevel:** A NETLOGON\_LOGON\_INFO\_CLASS structure, as specified in section [2.2.1.4.16](#Section_8c7808e54e5c420e9c9047286da2218f), that identifies the type of logon information in the *LogonInformation* union.

**LogonInformation:** A pointer to a [NETLOGON\_LEVEL](#Section_d0128545f74b4d89afd942621dff24c4) structure, as specified in section 2.2.1.4.6, that describes the logon information.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* The pointer contained in the *LogonInformation* parameter MUST not be NULL; otherwise, the server MUST return STATUS\_INVALID\_PARAMETER.
* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

The server MUST check the following parameters, and if any of them are NULL, it MUST return STATUS\_INVALID\_PARAMETER:

* *LogonServer*
* *ComputerName*
* *Authenticator*
* *ReturnAuthenticator*

The server MUST check the *LogonLevel* parameter, and the server MUST return STATUS\_INVALID\_INFO\_CLASS if it is not set to 1 (**NetlogonInteractiveInformation**).

If the request is not for the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) of which the server is a member and the server is a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), then the server MUST perform external behavior consistent with locally invoking **LsarQueryTrustedDomainInfoByName** ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.5), using the following parameters (policy handle is not needed locally):

* **TrustedDomainName** is set to the value of the *LogonInformation.LogonInteractive.Identity.LogonDomainName* parameter
* **InformationClass** is set to the value of **TrustedDomainInformationEx**.

If the call returns STATUS\_OBJECT\_NAME\_NOT\_FOUND (0xC0000034) the server MUST return STATUS\_NO\_SUCH\_DOMAIN. If the call returns any other error code other than STATUS\_SUCCESS the server MUST return that error code.

Additionally, the server MUST also verify that:

* The **securityIdentifier** (Sid) field ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.6.7.8) is not NULL,
* The **trustType** field ([MS-ADTS] section 6.1.6.7.15) is 1 or 2
* The **trustAttributes** field ([MS-ADTS] section 6.1.6.7.9) does not contain TRUST\_ATTRIBUTE\_UPLEVEL\_ONLY.

If **LsarQueryTrustedDomainInfoByName** succeeds and returns the domain information in *TrustedDomainInformation*, the server MUST check if it has established a secure channel with the domain. If there is not an established secure channel then the server MUST return the error code STATUS\_NO\_SUCH\_DOMAIN. If there is an established secure channel then the server MUST call NetrLogonSamLogoff using **LogonLevel** and **LogonInformation** to the DC with which it has established a secure channel.

Otherwise, if the server's account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) is for the domain specified by **LogonInformation.LogonInteractive.Identity.LogonDomainName**, then it MAY update the **lastLogoff** attribute ([[MS-ADA1]](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f) section 2.350) on the account object specified by the **LogonInformation.LogonInteractive.Identity.UserName** field.[<208>](#Appendix_A_208" \o "Product behavior note 208)

This method can only be called by a machine that has established a secure channel with the server.

#### Account Database Replication Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used for [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) replication as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NetrDatabaseDeltas (Opnum 7)

The NetrDatabaseDeltas method SHOULD[<209>](#Appendix_A_209" \o "Product behavior note 209) return a set of changes (or [**deltas**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e)) performed to the SAM, SAM built-in, or [**LSA databases**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b) after a particular value of the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d). It is used by BDCs to request [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) changes from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) that are missing on the BDC.

1. NTSTATUS NetrDatabaseDeltas(
2. [in, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD DatabaseID,
7. [in, out] PNLPR\_MODIFIED\_COUNT DomainModifiedCount,
8. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY\* DeltaArray,
9. [in] DWORD PreferredMaximumLength
10. );

**PrimaryName:** The custom binding handle (as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640)) that represents the connection to the PDC.

**ComputerName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the BDC calling this method.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure that contains the server return authenticator.

**DatabaseID:**  The identifier for a specific account database set as follows:

| Value | Meaning |
| --- | --- |
| 0x00000000 | Indicates the [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b). |
| 0x00000001 | Indicates the SAM built-in database. |
| 0x00000002 | Indicates the LSA database. |

**DomainModifiedCount:** A pointer to an NLPR\_MODIFIED\_COUNT structure, as specified in section [2.2.1.5.26](#Section_75dd36998abc45d29fb7e7a9a78779f5), that contains the database serial number. On input, this is the value of the database serial number on the client. On output, this is the value of the database serial number corresponding to the last element (delta) returned in the DeltaArray parameter.

**DeltaArray:** A pointer to a [NETLOGON\_DELTA\_ENUM\_ARRAY](#Section_82d47318c4d8458386a6ce186504bcba) structure that contains an array of enumerated changes (deltas) to the specified database with database serial numbers larger than the database serial number value specified in the input value of the *DomainModifiedCount* parameter.

**PreferredMaximumLength:** The value that specifies the preferred maximum size, in bytes, of data to return in the *DeltaArray* parameter. This is not a hard upper limit, but serves as a guide to the server. The server SHOULD[<210>](#Appendix_A_210" \o "Product behavior note 210) stop including elements in the returned *DeltaArray* after the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter. It is up to the client implementation to choose the value for this parameter.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The synchronization that this method performs is not a full synchronization; rather, a subset of database changes is returned. To perform a full synchronization, call [NetrDatabaseSync](#Section_86683ada19a2414eafaf124f77dc4685).

The server that receives this call MUST do the following:

* Verify that the client is a BDC.
* Verify the client authenticator. The server MUST return status code STATUS\_ACCESS\_DENIED if the verification fails.
* Validate that *DatabaseID* is one of the allowed values, 0x00000000 through 0x00000002. If the *DatabaseID* is not one of these values, the server MUST return the status code STATUS\_INVALID\_LEVEL.
* Given the BDC database serial number, obtain all database records that are missing on the BDC and return the array of deltas, NETLOGON\_DELTA\_ENUM\_ARRAY, for the missing records. The number of elements returned SHOULD be affected by the value of the *PreferredMaximumLength* parameter. The server SHOULD[<211>](#Appendix_A_211" \o "Product behavior note 211) stop including elements in the returned array after the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter. The server MAY also limit the number of elements per local configuration to avoid large array allocations.
* Compute and return the server authenticator.
* The server MUST set the value of the *DomainModifiedCount* parameter to the database serial number of the last delta returned in the array.
* If not all missing records are returned, the server MUST return the status code STATUS\_MORE\_ENTRIES.[<212>](#Appendix_A_212" \o "Product behavior note 212)

##### NetrDatabaseSync2 (Opnum 16)

The NetrDatabaseSync2 method SHOULD[<213>](#Appendix_A_213" \o "Product behavior note 213) return a set of all changes applied to the specified [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) since its creation. It provides an interface for a BDC to fully synchronize its databases to those of the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). Because returning all changes in one call might be prohibitively expensive due to a large amount of data being returned, this method supports retrieving portions of the database changes in a series of calls using a continuation context until all changes are received. It is possible for the series of calls to be terminated prematurely due to external events, such as system restarts. For that reason, the method also supports restarting the series of calls at a particular point specified by the caller. The caller MUST keep track of synchronization progress during the series of calls as detailed in this section.

1. NTSTATUS NetrDatabaseSync2(
2. [in, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD DatabaseID,
7. [in] SYNC\_STATE RestartState,
8. [in, out] ULONG \* SyncContext,
9. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY\* DeltaArray,
10. [in] DWORD PreferredMaximumLength
11. );

**PrimaryName:**  The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640), that represents the connection to the PDC.

**ComputerName:**  The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the BDC calling this method.

**Authenticator:**  A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:**  A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**DatabaseID:** The identifier for a specific database for which the changes are requested. It MUST be one of the following values.

| Value | Meaning |
| --- | --- |
| 0x00000000 | Indicates the [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b). |
| 0x00000001 | Indicates the SAM built-in database. |
| 0x00000002 | Indicates the [**LSA database**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b). |

**RestartState:** Specifies whether this is a restart of the series of the synchronization calls and how to interpret *SyncContext*. This value MUST be NormalState unless this is the restart, in which case the value MUST be set as specified in the description of the *SyncContext* parameter.

**SyncContext:** Specifies context needed to continue the operation. The value MUST be set to zero on the first call. The caller MUST treat this as an opaque value, unless this call is a restart of the series of synchronization calls. The value returned is to be used on input for the next call in the series of synchronization calls.

If this call is the restart of the series, the values of the *RestartState* and the *SyncContext* parameters are dependent on the **DeltaType** value received on the last call before the restart and MUST be set as follows. Find the last [NETLOGON\_DELTA\_ENUM](#Section_20e5863c014240f6a914f352a9d66047) structure in the *DeltaArray* parameter of the call. The **DeltaType** field of this NETLOGON\_DELTA\_ENUM structure, as specified in section 2.2.1.5.11, is the **DeltaType** needed for the restart. The values of *RestartState* and *SyncContext* are then determined from the following table.

| DeltaType | RestartState | SyncContext |
| --- | --- | --- |
| AddOrChangeGroup | GroupState | The value of the [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the last element |
| AddOrChangeUser | UserState | The value of the RID of the last element |
| ChangeGroupMembership | GroupMemberState | The value of the RID of the last element |
| AddOrChangeAlias | AliasState | 0x00000000 |
| ChangeAliasMembership | AliasMemberState | 0x00000000 |
| Any other value not previously listed | NormalState | 0x00000000 |

**DeltaArray:**  A pointer to a [NETLOGON\_DELTA\_ENUM\_ARRAY](#Section_82d47318c4d8458386a6ce186504bcba) structure, as specified in section 2.2.1.5.12, that contains an array of enumerated changes ([**deltas**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e)) to the specified database.

**PreferredMaximumLength:**  The value that specifies the preferred maximum size, in bytes, of data referenced in the *DeltaArray* parameter. This is not a hard upper limit, but serves as a guide to the server. The server SHOULD[<214>](#Appendix_A_214" \o "Product behavior note 214) stop including elements in the returned *DeltaArray* once the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter. It is up to the client implementation to choose the value for this parameter.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The server that receives this call MUST do the following:

* Verify that the client is a BDC, the server is a PDC, and is enabled. If any of these conditions are false, the server MUST return the status code STATUS\_NOT\_SUPPORTED.
* Apply Common Error Processing Rule B, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Validate that *DatabaseID* is one of the allowed values, 0x00000000 through 0x00000002. If the *DatabaseID* is not one of these values, the server MUST return the status code STATUS\_INVALID\_LEVEL.
* Given the *RestartState* parameter and the *SyncContext* parameter, obtain database records that are missing on the BDC and return the array of deltas, NETLOGON\_DELTA\_ENUM\_ARRAY, for the missing records. The number of elements returned SHOULD be affected by the value of the *PreferredMaximumLength* parameter. The server SHOULD[<215>](#Appendix_A_215" \o "Product behavior note 215) stop including elements in the returned array once the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter. The server MAY also limit the number of elements per local configuration to avoid large array allocations.
* The server MUST update and return the *SyncContext* parameter (section [2.2.1.5.29](#Section_ffce9bbc6ae544788f45e82c3847aaa2)) to continue the synchronization loop on the next client request.
* Compute and return the server authenticator.
* Initialize **SynchronizationComplete** by setting it to FALSE, and when all the missing records are sent set **SynchronizationComplete** to TRUE.
* If **SynchronizationComplete** is FALSE, the server MUST return the status code STATUS\_MORE\_ENTRIES.

##### NetrDatabaseSync (Opnum 8)

The NetrDatabaseSync method[<216>](#Appendix_A_216" \o "Product behavior note 216) is a predecessor to the [NetrDatabaseSync2](#Section_31fc80bd4f4d4512a792e488bb78f6a0) method (section 3.5.4.6.2). All parameters of this method have the same meanings as the identically named parameters of the NetrDatabaseSync2 method.

1. NTSTATUS NetrDatabaseSync(
2. [in, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD DatabaseID,
7. [in, out] ULONG \* SyncContext,
8. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY\* DeltaArray,
9. [in] DWORD PreferredMaximumLength
10. );

Receiving this method is identical to receiving NetrDatabaseSync2, as specified in section 3.5.4.6.2, except that this call does not use the *RestartState* parameter. NetrDatabaseSync does not support restarting the synchronization loop.

##### NetrDatabaseRedo (Opnum 17)

The NetrDatabaseRedo method SHOULD[<217>](#Appendix_A_217" \o "Product behavior note 217) be used by a BDC to request information about a single account from the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d).

1. NTSTATUS NetrDatabaseRedo(
2. [in, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in, size\_is(ChangeLogEntrySize)]
7. UCHAR \* ChangeLogEntry,
8. [in] DWORD ChangeLogEntrySize,
9. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY\* DeltaArray
10. );

**PrimaryName:** The custom binding handle, defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640), representing the connection to the PDC.

**ComputerName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the BDC calling this method.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**ChangeLogEntry:** A pointer to a buffer that contains a CHANGELOG\_ENTRY structure, specified as follows, for the account being queried.

**ChangeLogEntrySize:** The size, in bytes, of the buffer pointed to by the *ChangeLogEntry* parameter.

**DeltaArray:** A pointer to a [NETLOGON\_DELTA\_ENUM\_ARRAY](#Section_82d47318c4d8458386a6ce186504bcba) structure, as specified in section 2.2.1.5.12, that contains an array of enumerated [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) changes for the account being queried.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The following CHANGELOG\_ENTRY structure pointed to by the *ChangeLogEntry* parameter carries information about the account object being queried.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| SerialNumber [0..3] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SerialNumber [4..7] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectRid | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Flags | | | | | | | | | | | | | | | | DBIndex | | | | | | | | DeltaType | | | | | | | |
| ObjectSid (optional, variable length) … | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ObjectName (optional, variable length) … | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

**SerialNumber:** The [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) that corresponds to this account object (64-bit integer).

**ObjectRid:** The [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the object (32-bit integer).

**Flags:** A two-byte set of bit flags that describes the properties of the message. A flag is TRUE (or set) if its value is equal to 1. The value is constructed from zero or more bit flags from the following table, with the exception that bit C cannot be combined with bit D.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | E | D | C | B | A |

The flags are defined as follows.

| Flag | Meaning |
| --- | --- |
| A | The object requires immediate replication at the moment that the object is changed. |
| B | The object is an account with a changed password. |
| C | The optional **ObjectSid** field is included in the message. Cannot be combined with flag D. |
| D | The optional **ObjectName** field is included in the message. Cannot be combined with flag C. |
| E | The object is the first object changed after a promotion of a BDC to a new PDC. |

All other bits MUST be set to zero and MUST be ignored on receipt.

**DBIndex:** The 8-bit integer identifier of the database containing the object. MUST be one, and only one, of the following values.

| Value | Meaning |
| --- | --- |
| 0x00 | The [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b). |
| 0x01 | The SAM built-in database. |
| 0x02 | The [**LSA database**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b). |

**DeltaType:** One of the [NETLOGON\_DELTA\_TYPE](#Section_f8a8cd32426d45f1be45e0dc5c1c1359) values specified in section 2.2.1.5.28.

**ObjectSid:** The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) of the object. Included only if flag C is set. This is an RPC\_SID structure, as defined in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) section 2.4.2.3.

**ObjectName:** The name of the object. **ObjectName** is a null-terminated Unicode string, and is included only if flag D is set.

The server that receives this call MUST do the following:

* Verify that the client is a BDC, the server is a PDC, and synchronization is enabled. If any of these conditions are false, the server MUST return the status code STATUS\_NOT\_SUPPORTED.
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Validate the *ChangeLogEntry* parameter as a valid single account object information request message. If the *ChangeLogEntry* parameter is not valid, the server MUST return the status code STATUS\_INVALID\_PARAMETER.

The server uses the server name passed in the *PrimaryName* parameter to look up the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) that the server hosts. If the name is not found, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME.

Return a single [**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e) for the requested account in the *DeltaArray* parameter.

#### Domain Trust Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used to retrieve [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) data, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### DsrEnumerateDomainTrusts (Opnum 40)

The DsrEnumerateDomainTrusts method SHOULD[<218>](#Appendix_A_218" \o "Product behavior note 218) return an enumerated list of [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6), filtered by a set of flags, from the specified server.

1. NET\_API\_STATUS DsrEnumerateDomainTrusts(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] ULONG Flags,
4. [out] PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY Domains
5. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**Flags:** A set of bit flags that specify properties that MUST be true for a domain trust to be part of the returned [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) list. A flag is TRUE (or set) if its value is equal to 1. Flags MUST contain one or more of the following bits.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | F | E | D | C | B | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Domain is a member of the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62). |
| B | Domain is directly trusted by this domain. |
| C | Domain is the root of a [**domain tree**](#gt_e2c071f1-5977-4749-868f-6c5a04929476) in the forest. |
| D | Domain is the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) of the queried server. |
| E | Primary domain is running in native mode. |
| F | Domain directly trusts this domain. |

All other bits MUST be set to zero.

**Domains:** A pointer to a [NETLOGON\_TRUSTED\_DOMAIN\_ARRAY](#Section_251cf1be29324d338532595cf42e8091) structure, as specified in section 2.2.1.6.3, that contains a list of trusted domains.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns one of the following error codes.

| Return Value/Code | Description |
| --- | --- |
| 0x0000051F  ERROR\_NO\_LOGON\_SERVERS | There are currently no logon servers available to service the logon request. |
| 0x000006FA  ERROR\_NO\_TRUST\_LSA\_SECRET | The workstation does not have a trust secret. |
| 0x000006FB  ERROR\_NO\_TRUST\_SAM\_ACCOUNT | The security [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) on the server does not have a computer account for this workstation trust relationship. |

On receiving this call, the server MUST perform the following validation step:

* The *Flags* parameter MUST be checked to verify that at least one of the valid bits is set. All other bits (0-24) MUST be zero. The server MUST return ERROR\_INVALID\_FLAGS if there are invalid bits present.

If the *ServerName* parameter is not NULL, it is compared against the server's [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b). If the *ServerName* parameter does not match the server's computer name, the server MUST return ERROR\_INVALID\_COMPUTERNAME. If the *ServerName* parameter matches the server's computer name or the *ServerName* parameter is NULL, then processing proceeds.

If the server is not a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) (section [3.1.4.8](#Section_16f8294280d643ac8c38eee3cfe4ac99)), the server SHOULD call [NetrLogonGetDomainInfo](#Section_7c3ad0ccee054643b7734d84e1d431dc) to a DC in its domain, with the following parameters:

* The *NetlogonWorkstationInfo* parameter with the following elements:
  + *NetlogonWorkstationInfo.LsaPolicy.LsaPolicySize* is set to 0.
  + *NetlogonWorkstationInfo.LsaPolicy.LsaPolicy* is set to NULL.
  + *NetlogonWorkstationInfo.WorkStationFlags* has the A flag set.
  + *NetlogonWorkstationInfo.DnsHostName* set to the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) computer name.
* Level MUST be set to 0x1.

If the server is a domain controller (section 3.1.4.8), it MUST perform behavior equivalent to locally invoking NetrLogonGetDomainInfo with the previously described parameters.

If the call returns any other error code other than STATUS\_SUCCESS, then the server MUST return that error code and no further processing occurs.

If the call returns STATUS\_SUCCESS, the server MUST use the returned domains in the DomBuffer.TrustedDomains parameter to build and return an array of **DS\_DOMAIN\_TRUSTSW** structures from the **NETLOGON\_ONE\_DOMAIN\_INFO** structures as follows:

* If the primary domain is determined to not be running in [**mixed mode**](#gt_06c1c70e-f2c6-4efd-bff8-474409e69660) ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.4.1), and the E bit is set in the *Flags* parameter, the server MUST include the primary domain (*DomBuffer.PrimaryDomain*) in the returned array.
* For each element of *DomBuffer.TrustedDomains*, if the bitwise AND of the *Flags* parameter and the *DomBuffer.TrustedDomains.TrustExtension.Flags* (*Flags* & *DomBuffer.TrustedDomains.TrustExtension[0-3]*) is true, the server MUST include the domain in the returned array.
* For each element to be included in the returned array, each field in the NETLOGON\_ONE\_DOMAIN\_INFO structure listed in the first column of the following table is copied to the field of the DS\_DOMAIN\_TRUSTSW structure listed on the same line in the second column:

| NETLOGON\_ONE\_DOMAIN\_INFO element | DS\_DOMAIN\_TRUSTSW element |
| --- | --- |
| DomainName | NetBiosDomainName |
| DnsDomainName | DnsDomainName |
| DomainGuid | DomainGuid |
| DomainSid | DomainSid |
| Bytes 0 – 3 of TrustExtension | Flags |
| Bytes 4 – 7 of TrustExtension | ParentIndex |
| Bytes 8 – 11 of TrustExtension | TrustType |
| Bytes 12 – 15 of Trust Extension | TrustAttributes |

##### NetrEnumerateTrustedDomainsEx (Opnum 36)

The NetrEnumerateTrustedDomainsEx method SHOULD[<219>](#Appendix_A_219" \o "Product behavior note 219) return a list of [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) from a specified server. This method extends NetrEnumerateTrustedDomains by returning an array of domains in a more flexible [DS\_DOMAIN\_TRUSTSW](#Section_7de9866ed3ef4a9f98a5c2dcff1e61c1) structure, as specified in section 2.2.1.6.2, rather than the array of strings in [DOMAIN\_NAME\_BUFFER](#Section_11743dc47a2d4464b35150aeb8801b8b) structure, as specified in section 2.2.1.6.1. The array is returned as part of the [NETLOGON\_TRUSTED\_DOMAIN\_ARRAY](#Section_251cf1be29324d338532595cf42e8091) structure, as specified in section 2.2.1.6.3.

1. NET\_API\_STATUS NetrEnumerateTrustedDomainsEx(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [out] PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY Domains
4. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**Domains:** A pointer to a NETLOGON\_TRUSTED\_DOMAIN\_ARRAY structure, as specified in section 2.2.1.6.3, that contains an array of DS\_DOMAIN\_TRUSTSW structures, as specified in section 2.2.1.6.2, one for each trusted domain.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns one of the following error codes.

| Return Value/Code | Description |
| --- | --- |
| 0x0000051F  ERROR\_NO\_LOGON\_SERVERS | There are currently no logon servers available to service the logon request. |
| 0x000006FA  ERROR\_NO\_TRUST\_LSA\_SECRET | The workstation does not have a trust secret. |
| 0x000006FB  ERROR\_NO\_TRUST\_SAM\_ACCOUNT | The security [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) on the server does not have a computer account for this workstation trust relationship. |

This method is a wrapper for [DsrEnumerateDomainTrusts](#Section_f98236242b34415cbdca9f9a6d97016b), which strips off the F flag from the returned data for backward compatibility. For details, see section 3.5.4.7.1.

##### NetrEnumerateTrustedDomains (Opnum 19)

The NetrEnumerateTrustedDomains method SHOULD[<220>](#Appendix_A_220" \o "Product behavior note 220) return a set of [**NetBIOS names**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) [**domains**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. NTSTATUS NetrEnumerateTrustedDomains(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [out] PDOMAIN\_NAME\_BUFFER DomainNameBuffer
4. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**DomainNameBuffer:** A pointer to a [DOMAIN\_NAME\_BUFFER](#Section_11743dc47a2d4464b35150aeb8801b8b) structure, as specified in section 2.2.1.6.1, that contains a list of trusted [**domain names**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c). The format of domain names contained in the buffer is specified in section 2.2.1.6.1.

**Return Values:** The method returns 0x00000000 on success; otherwise, it SHOULD return one of the following error codes.

| Return Value/Code | Description |
| --- | --- |
| 0x0000051F  ERROR\_NO\_LOGON\_SERVERS | There are currently no logon servers available to service the logon request. |
| 0x000006FA  ERROR\_NO\_TRUST\_LSA\_SECRET | The workstation does not have a trust secret. |
| 0x000006FB  ERROR\_NO\_TRUST\_SAM\_ACCOUNT | The security [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) on the server does not have a computer account for this workstation trust relationship. |

The server initializes the *DomainNames* field of the DOMAIN\_NAME buffer to the empty string. The server calls the [NetrEnumerateTrustedDomainsEx](#Section_c3e9870a09434d45be94edb9419a1c11) method and for each **PDS\_DOMAIN\_TRUSTSW** element of the **NETLOGON\_TRUSTED\_DOMAIN\_ARRAY**, appends the *NetbiosDomainName* field to the *DomainNames* field of the **DOMAIN\_NAME\_BUFFER** (section 2.2.1.6.1). Then the server terminates the *DomainNames* field with two null bytes.

For details, see section 3.5.4.7.2, Receiving NetrEnumerateTrustedDomainsEx.

##### NetrGetForestTrustInformation (Opnum 44)

The NetrGetForestTrustInformation method SHOULD[<221>](#Appendix_A_221" \o "Product behavior note 221) retrieve the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) information for the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) of which the member's [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) is itself a member.

1. NTSTATUS NetrGetForestTrustInformation(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD Flags,
7. [out] PLSA\_FOREST\_TRUST\_INFORMATION\* ForestTrustInfo
8. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the client computer [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf).

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**Flags:** MUST be set to zero and MUST be ignored on receipt.

**ForestTrustInfo:** A pointer to an LSA\_FOREST\_TRUST\_INFORMATION structure, as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.7.25, that contains data for each [**forest trust**](#gt_035d9ce5-f117-4251-8d4d-127c462ec4a0).

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.
* Ensure that the caller is a [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in a different domain by checking that the *SecureChannelType* from ChallengeTable is TrustedDnsDomainSecureChannel or TrustedDomainSecureChannel. For all other types, this call MUST return STATUS\_NOT\_IMPLEMENTED.
* Apply Common Error Processing Rule B, specified in section 3, to the *ServerName* parameter.

The [**forest trust information**](#gt_8c0b82d9-efec-4723-95a9-8564edf9ba44) for the domain hosted by *ServerName* MUST be returned.

This method can only be called by a machine that has established a secure channel with the server.

##### DsrGetForestTrustInformation (Opnum 43)

The DsrGetForestTrustInformation method SHOULD[<222>](#Appendix_A_222" \o "Product behavior note 222) retrieve the [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) information for the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) of the specified [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), or for a forest trusted by the forest of the specified DC.

1. NET\_API\_STATUS DsrGetForestTrustInformation(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, unique, string] wchar\_t\* TrustedDomainName,
4. [in] DWORD Flags,
5. [out] PLSA\_FOREST\_TRUST\_INFORMATION\* ForestTrustInfo
6. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**TrustedDomainName:** The optional null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the trusted [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) for which the [**forest trust information**](#gt_8c0b82d9-efec-4723-95a9-8564edf9ba44) is to be gathered.

**Flags:** A set of bit flags that specify additional applications for the forest trust information. A flag is TRUE (or set) if its value is equal to 1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | A |

Where the bits are defined as:

| Value | Description |
| --- | --- |
| A | Update a [**trusted domain object (TDO)**](#gt_f2ceef4e-999b-4276-84cd-2e2829de5fc4) with the information returned in ForestTrustInfo. |

All other bits MUST be set to zero.

**ForestTrustInfo:** A pointer to an LSA\_FOREST\_TRUST\_INFORMATION structure, as specified in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.7.25, that contains data for each [**forest trust**](#gt_035d9ce5-f117-4251-8d4d-127c462ec4a0).

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns the following error code.

| Return Value/Code | Description |
| --- | --- |
| 0x00000001  ERROR\_INVALID\_FUNCTION | Incorrect function. |

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Apply Common Error Processing Rule B, specified in section 3.
* Verify that the client has sufficient [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940). The server SHOULD determine if the client has sufficient privileges (as specified in section 3.5.4.1) with the Access Request mask set to match the NETLOGON\_FTINFO\_ACCESS mask; otherwise, the server MUST return ERROR\_ACCESS\_DENIED.
* Verify that if the *Flags* parameter has bit A enabled, the server is a PDC; otherwise, the server MUST return NERR\_NotPrimary.
* The *Flags* parameter MUST be checked for invalid bit flags. The server MUST return ERROR\_INVALID\_FLAGS if any bit other than A is set.

If the *TrustedDomainName* parameter is specified, the server calls the DsrGetForestTrustInformation method on a DC in the trusted domain specified by the *TrustedDomainName* parameter.

Additionally, if the *TrustedDomainName* is not NULL, the server MUST perform the additional following validation steps:

* Verify that the server has established a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) with the domain specified in the *TrustedDomainName* parameter, and apply Common Error Processing Rule E, specified in section 3. If the server has not established a secure channel with the domain specified in the *TrustedDomainName* parameter, then the server MUST return the error code ERROR\_NO\_SUCH\_DOMAIN.
* Apply Common Error Processing Rule C, specified in section 3.
* The forest trust information for the domain specified by the *TrustedDomainName* parameter MUST be returned.
* The server MUST verify that the *TrustedDomainName* refers to a cross-forest trust by performing external behavior consistent with locally invoking LsarQueryTrustedDomainInfoByName ([MS-LSAD] section 3.1.4.7.5), using the following parameters (a policy handle is not needed locally):
  + *Domain* is set to the value of the *TrustedDomainName* parameter
  + *InformationClass* is set to the value of TrustedDomainInformationEx.

If the call returns STATUS\_OBJECT\_NAME\_NOT\_FOUND the server MUST return ERROR\_NO\_SUCH\_DOMAIN. Additionally, the server MUST verify that:

* + The **securityIdentifier** (Sid) field ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.1.6.7.8) is not NULL
  + The **trustType** field ([MS-ADTS] section 6.1.6.7.15) is 1 or 2
  + The **trustAttributes** field ([MS-ADTS] section 6.1.6.7.9) does not contain TRUST\_ATTRIBUTE\_UPLEVEL\_ONLY
  + The **trustAttributes** field ([MS-ADTS] section 6.1.6.7.9) contains TRUST\_ATTRIBUTE\_FOREST\_TRANSITIVE.

If the server fails to verify any of the preceding conditions, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

Otherwise, if the *TrustedDomainName* is NULL, the server MUST check to see if Flags bit A is set. If Flags bit A is set, the server MUST return ERROR\_INVALID, and no further processing occurs.

The server MUST retrieve the forest trust information for the domain specified by the TrustedDomainName parameter:

* If the *TrustedDomainName* is NULL the server SHOULD perform external behavior equivalent to locally invoking NetrGetForestTrustInformation with the parameters specified in the previous paragraph, return the forest trust information, and stop further processing.
* Otherwise, the server SHOULD call NetrGetForestTrustInformation with the following parameters (in addition to those specified in section [3.4.5.5.4](#Section_c7308656b404469fb976947ae0ae2370)) to a [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d), in the domain specified by the *TrustedDomainName* Parameter, in order to retrieve the Trusted Forest's version of the LSA\_FOREST\_TRUST\_INFORMATION, referred to in the rest of this section as NewTrustInfo:
  + **ServerName** is set to NULL, indicating the current server's domain.
  + **ComputerName** is set to the NetBIOS [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b) of the server.
  + **Flags** is set to 0.

Otherwise, if the *TrustedDomainName* is not NULL and Flags bit A is set, the server SHOULD update the server's forest information for the domain specified by the *TrustedDomainName* parameter as follows:

* The server MUST retrieve its version of the forest trust information, referred to in the rest of this section as OldTrustInfo, by performing external behavior equivalent to locally invoking LsarQueryForestTrustInformation with the following parameters (a policy handle is not required locally):
  + **TrustedDomainName** is set to the *TrustedDomainName* parameter that was passed by the caller of DsrGetForestTrustInformation
  + **HighestRecordType** is set to ForestTrustRecordTypeLast.
* If the call returns STATUS\_NOT\_FOUND, the server SHOULD ignore this error and continue processing. If any other error is returned, the server SHOULD pass the error through and stop processing.
* The server SHOULD merge the OldTrustInfo LSA\_FOREST\_TRUST\_INFORMATION with the Trusted Forest's version of the NewTrustInfo LSA\_FOREST\_TRUST\_INFORMATION. The server SHOULD create an LSA\_FOREST\_TRUST\_INFORMATION structure. After the merge the new version of the LSA\_FOREST\_TRUST\_INFORMATION will result in the merged result, referred to in this section as MergedTrustInfo. The server SHOULD perform the merge using the following rules:
  + The server SHOULD iterate through the LSA\_FOREST\_TRUST\_RECORD ([MS-LSAD] section 2.2.7.21) entries in the NewTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in NewTrustInfo.Entries is denoted as "i":
    - If the NewTrustInfo.Entries[i].ForestTrustType is not ForestTrustTopLevelName, then ignore further rules for NewTrustInfo.Entries[i], and continue iterating through NewTrustInfo.Entries.
    - If the NewTrustInfo.Entries[i].ForestTrustData.TopLevelName is equal to the DNS [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) of the TDO, copy NewTrustInfo.Entries[i] into MergedTrustInfo.Entries, ignore further rules for NewTrustInfo.Entries[i], and continue iterating through NewTrustInfo.Entries.
    - Iterate through the LSA\_FOREST\_TRUST\_RECORD entries in the MergedTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in MergedTrustInfo.Entries is denoted as "m":
      * If the NewTrustInfo.Entries[i].ForestTrustData.TopLevelName is subordinate to the MergedTrustInfo.Entries[m].ForestTrustData.TopLevelName, stop iterating through MergedTrustInfo.Entries, ignore further rules for NewTrustInfo.Entries[i], and continue iterating through NewTrustInfo.Entries.
    - Copy the NewTrustInfo.Entries[i] to MergedTrustInfo.Entries. The new entry in MergedTrustInfo.Entries is referred to as MergedEntry.
      * Iterate through the LSA\_FOREST\_TRUST\_RECORD entries in the OldTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in OldTrustInfo.Entries is denoted as "k":
        + If the OldTrustInfo.Entries[k].ForestTrustType is equal to ForestTrustTopLevelName, and the NewTrustInfo.Entries[i].ForestTrustData.TopLevelName is equal to OldTrustInfo.Entries[k].ForestTrustData.TopLevelName, copy OldTrustInfo.Entries[k].Flags to MergedEntry.Flags and copy OldTrustInfo.Entries[k].Time to MergedEntry.Time.
        + Otherwise, MergedEntry.Flags is set to LSA\_TLN\_DISABLED\_NEW and MergedEntry.Time is set to 0.
  + The server SHOULD iterate through the LSA\_FOREST\_TRUST\_RECORD ([MS-LSAD] section 2.2.7.21) entries in the NewTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in NewTrustInfo.Entries is denoted as "i":
    - If the NewTrustInfo.Entries[i].ForestTrustType is a ForestTrustDomainInfo, create a new LSA\_FOREST\_TRUST\_RECORD, referred to in this section as TempEntry, and copy NewTrustInfo.Entries[i] into TempEntry. TempEntry.Flags is set to 0 and TempEntry.Time is set to 0.
    - Iterate through the LSA\_FOREST\_TRUST\_RECORD entries in the MergedTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in MergedTrustInfo.Entries is denoted as "m":
      * If MergedTrustInfo.Entries[m].ForestTrustType is a ForestTrustDomainInfo and TempEntry.ForestTrustData.DomainInfo.Sid is equal to MergedTrustInfo.Entries[m].ForestTrustData.DomainInfo.Sid, delete TempEntry, stop iterating through MergedTrustInfo.Entries, ignore further rules for NewTrustInfo.Entries[i], and continue iterating through NewTrustInfo.Entries.
      * Iterate through the LSA\_FOREST\_TRUST\_RECORD Entries in the OldTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in OldTrustInfo.Entries is denoted as "n":
        + If OldTrustInfo.Entries[n].ForestTrustType is a ForestTrustDomainInfo and TempEntry.ForestTrustData.DomainInfo.NetbiosName is equal to OldTrustInfo.Entries[n].ForestTrustData.DomainInfo.NetbiosName, copy OldTrustInfo.Entries[n].Flags into TempEntry.Flags and also copy OldTrustInfo.Entries[n].Time into TempEntry.Time.
    - Copy TempEntry into MergedTrustedInfo.Entries.
  + The server SHOULD iterate through the LSA\_FOREST\_TRUST\_RECORD ([MS-LSAD] section 2.2.7.21) entries in the OldTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in OldTrustInfo.Entries is denoted as "i":
    - If OldTrustInfo.Entries[i].ForestTrustType is not ForestTrustDomainInfo, then ignore further rules for OldTrustInfo.Entries[i] and continue iterating through OldTrustInfo.Entries.
    - Iterate through the LSA\_FOREST\_TRUST\_RECORD entries in the MergedTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in MergedTrustInfo.Entries is denoted as "m":
      * If MergedTrustInfo.Entries[m].ForestTrustType is a ForestTrustDomainInfo and OldTrustInfo.Entries[m].ForestTrustData.DomainInfo.NetbiosName equals MergedTrustInfo.Entries[m].ForestTrustData.DomainInfo.NetbiosName, stop iterating through the MergedTrustInfo.Entries, ignore further rules for OldTrustInfo.Entries[i] and continue iterating through OldTrustInfo.Entries.
    - If OldTrustInfo.Entries[i].Flags has either the LSA\_SID\_DISABLED\_ADMIN flag set or the LSA\_NB\_DISABLED\_ADMIN flag set, copy OldTrustInfo.Entries[i] into MergedTrustInfo.Entries.
  + The server SHOULD iterate through the LSA\_FOREST\_TRUST\_RECORD ([MS-LSAD] section 2.2.7.21) entries in the OldTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in OldTrustInfo.Entries is denoted as "i":
    - If OldTrustInfo.Entries[i].ForestTrustType is not equal to ForestTrustTopLevelNameEx, then ignore further rules for OldTrustInfo.Entries[i] and continue iterating through OldTrustInfo.Entries.
    - Iterate through the LSA\_FOREST\_TRUST\_RECORD entries in the MergedTrustInfo version of the LSA\_FOREST\_TRUST\_INFORMATION according to the following rules. The index for the current entry in MergedTrustInfo.Entries is denoted as "m":
      * If MergedTrustInfo.Entries[m].ForestTrustType is a ForestTrustTopLevelName and OldTrustInfo.Entries[i].ForestTrustData.TopLevelName is equal to or subordinate to MergedTrustInfo.Entries[m].ForestTrustData.TopLevelName, copy OldTrustInfo.Entries[i] into MergedTrustInfo.Entries. Stop iterating through MergedTrustInfo.Entries, but continue iterating through OldTrustInfo.Entries.

The server MUST update its version of the forest trust information for the domain specified by the TrustedDomainName parameter by performing external behavior equivalent to locally invoking LsarSetForestTrustInformation, with the following parameters (a policy handle is not needed locally):

* **TrustedDomainName** is set to the TrustedDomainName parameter that was passed by the caller of DsrGetForestTrustInformation
* **HighestRecordType** is set to ForestTrustRecordTypeLast
* **ForestTrustInfo** is set to the merged forest trust information, MergedTrustInfo.

If the *TrustedDomainName* is NULL:

* The forest trust information for the domain hosted by *ServerName* MUST be returned if *Flags* bit A is not set.
* The server MUST return ERROR\_INVALID\_FLAGS if *Flags* bit A is set.

##### NetrServerGetTrustInfo (Opnum 46)

The NetrServerGetTrustInfo method SHOULD[<223>](#Appendix_A_223" \o "Product behavior note 223) return an information block from a specified server. The information includes encrypted current and previous passwords for a particular account and additional [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) data. The account name requested MUST be the name used when the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) was created, unless the method is called on a [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) by a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), in which case it can be any valid account name.

1. NTSTATUS NetrServerGetTrustInfo(
2. [in, unique, string] LOGONSRV\_HANDLE TrustedDcName,
3. [in, string] wchar\_t\* AccountName,
4. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
5. [in, string] wchar\_t\* ComputerName,
6. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
7. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
8. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNewOwfPassword,
9. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedOldOwfPassword,
10. [out] PNL\_GENERIC\_RPC\_DATA\* TrustInfo
11. );

**TrustedDcName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**AccountName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the client account in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

**SecureChannelType:**  A [NETLOGON\_SECURE\_CHANNEL\_TYPE](#Section_4d1235e32c964e9fa1473cb338a0d09f) enumerated value, as specified in section 2.2.1.3.13, that indicates the type of the secure channel being established by this call.

**ComputerName:** The null-terminated Unicode string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer, for which the trust information MUST be returned.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**EncryptedNewOwfPassword:** A pointer to an [ENCRYPTED\_NT\_OWF\_PASSWORD](#Section_f7458576d53847cdb387b6f98449a0ee) structure, as specified in [[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 2.2.3.3, that contains the NTOWFv1 (as specified in NTLM v1 Authentication in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of the current password, encrypted as specified in [MS-SAMR] section 2.2.11.1.1, Encrypting an NT Hash or LM Hash Value with a specified key. The [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) is the specified 16-byte key that is used to derive its keys via the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4.

**EncryptedOldOwfPassword:** A pointer to an ENCRYPTED\_NT\_OWF\_PASSWORD structure, as specified in [MS-SAMR] section 2.2.3.3, that contains the NTOWFv1 (as specified in NTLM v1 Authentication in [MS-NLMP] section 3.3.1) of the old password, encrypted as specified in [MS-SAMR] section 2.2.11.1.1, Encrypting an NT Hash or LM Hash Value with a specified key. The session key is the specified 16-byte key that is used to derive its keys via the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4.

**TrustInfo:** A pointer to an [NL\_GENERIC\_RPC\_DATA](#Section_a1c7f3cac8b145149fd5ed3460c83a4d) structure, as specified in section 2.2.1.6.4, that contains a block of generic [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) data with trust information for the specified server.

**Return Values:** The method returns 0x00000000 to indicate success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the secure channel to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

If the *TrustedDcName* parameter is not NULL, it is compared against the server's [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b). If the *TrustedDcName* parameter does not match the server's computer name, or is NULL, then the server MUST return STATUS\_INVALID\_COMPUTER\_NAME. If the *TrustedDcName* parameter matches the server's computer name, processing proceeds.

The server MUST retrieve the [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of the current password for the account identified by the *AccountName* and *SecureChannelType* parameters. If the *SecureChannelType* is **TrustedDnsDomainSecureChannel** or **TrustedDomainSecureChannel**, then the SharedSecret of the trust will be used and the OWF of the previous password MUST also be retrieved. All other types of *SecureChannelType* require that the SharedSecret of the computer account be used, and that an empty string MUST be used when calculating the OWF of the previous password.

The NTOWFv1 of the current and previous passwords MUST be encrypted as specified in [MS-SAMR] section 2.2.11.1.1, Encrypting an NT Hash or LM Hash Value with a specified key. The session key is the specified 16-byte key used to derive its keys via the 16-byte value process, as specified in [MS-SAMR] section 2.2.11.1.4. The encrypted versions of the NTOWFv1 for the current password and previous password MUST be returned in the parameters *EncryptedNewOwfPassword* and *EncryptedOldOwfPassword*, respectively.

If the *TrustInfo* parameter is not NULL, the structure is generated by setting NL\_GENERIC\_RPC\_DATA.UlongEntryCount to 1 and setting NL\_GENERIC\_RPC\_DATA.UlongData to a 32-bit value that contains the trust attributes. The trust attributes themselves are defined in [[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 2.2.7.9 as the TrustAttributes member, as part of the LSAPR\_TRUSTED\_DOMAIN\_INFORMATION\_EX structure.

This method can only be called by a machine that has established a secure channel with the server.

#### Message Protection Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used by components outside Netlogon to accomplish certain tasks, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NetrLogonGetTrustRid (Opnum 23)

The NetrLogonGetTrustRid method SHOULD[<224>](#Appendix_A_224" \o "Product behavior note 224) be used to obtain the [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the account whose password is used by [**domain controllers**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) for establishing the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) from the server receiving this call.

1. NET\_API\_STATUS NetrLogonGetTrustRid(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string, unique] wchar\_t\* DomainName,
4. [out] ULONG \* Rid
5. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**DomainName:** The null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the primary or [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain. If this parameter is NULL, this method uses the name of the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) of the server.

**Rid:** A pointer to an unsigned long that receives the RID of the account.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The server SHOULD[<225>](#Appendix_A_225" \o "Product behavior note 225) return ERROR\_ACCESS DENIED if the caller is not local.

If *ServerName* equals NULL and *DomainName* equals NULL, then the server SHOULD determine if the client has sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940) (as described in section [3.5.4.2](#Section_1ec948862b6445afb68e3d9faa36617c)) with the Access Request mask set to NETLOGON\_FTINFO\_ACCESS.

Otherwise, the server SHOULD determine if the client has sufficient privilege (as described in section 3.5.4.2) with the Access Request mask set to NETLOGON\_SERVICE\_ACCESS.

If the client does not have sufficient privilege, the server MUST return ERROR\_ACCESS\_DENIED.

If *ServerName* equals NULL, then the call MUST be made to the local machine. If the *DomainName* is the same as the domain that the machine is joined to, the call MUST succeed, and the server MUST return the **AccountRid** of the machine in the domain. If the *DomainName* is a different domain, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.

If both *ServerName* and *DomainName* are NULL, the server MUST return the RID for the computer account of the caller. Otherwise, the RID for the account identified by *ServerName* and *DomainName* MUST be returned.

The server uses the server name passed in the *ServerName* parameter to look up the domain for the request. If the name is not found, the server MUST return ERROR\_INVALID\_COMPUTERNAME.

If the RID cannot be determined, the server SHOULD return ERROR\_TRUSTED\_RELATIONSHIP\_FAILURE.

##### NetrLogonComputeServerDigest (Opnum 24)

The NetrLogonComputeServerDigest method computes a cryptographic digest of a message by using the MD5 message-digest algorithm, as specified in [[RFC1321]](https://go.microsoft.com/fwlink/?LinkId=90275). This method SHOULD[<226>](#Appendix_A_226" \o "Product behavior note 226) be called by a client computer against a server and is used to compute a message digest, as specified in this section. The client can then call the [NetrLogonComputeClientDigest](#Section_79ca6e90ccd2429eb5ac8050b620eef6) method (as specified in section [3.4.5.6.3](#Section_1bf3702bbe13464aad5e6be0fe210c90)) and compare the digests to ensure that the server that it communicates with knows the [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) between the client machine and the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. NET\_API\_STATUS NetrLogonComputeServerDigest(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] ULONG Rid,
4. [in, size\_is(MessageSize)] UCHAR \* Message,
5. [in] ULONG MessageSize,
6. [out] CHAR NewMessageDigest[16],
7. [out] CHAR OldMessageDigest[16]
8. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**Rid:** The [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) of the machine account for which the digest is to be computed. The [NetrLogonGetTrustRid method](#Section_1d6fad9e763d495f9bed18c79304c3d7), as specified in section 3.5.4.8.1, is used to obtain the RID.

**Message:** A pointer to buffer that contains the message to compute the digest.

**MessageSize:** The length of the data referenced by the *Message* parameter, in bytes.

**NewMessageDigest:** A 128-bit MD5 digest of the current machine account password and the message in the *Message* buffer. The machine account is identified by the *Rid* parameter.

**OldMessageDigest:** A 128-bit MD5 digest of the previous machine account password, if present, and the message in the *Message* buffer. If no previous machine account password exists, then the current password is used. The machine account is identified by the *Rid* parameter.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The server uses the server name passed in the *ServerName* parameter to look up the domain for the request. If the name is not found, the server MUST return ERROR\_INVALID\_COMPUTERNAME.

If the client does not have sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940), the server MUST return ERROR\_ACCESS\_DENIED.

The server MUST construct the machine account [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) using the *Rid* parameter and the current domain with the format S-1-5-*current domain*-*Rid parameter*.

The server MUST compute or retrieve the NTOWFv1 of the current password, retrieve **lmPwdHistory** ([[MS-ADA1]](%5bMS-ADA1%5d.pdf#Section_19528560f41e4623a406dabcfff0660f) section 2.363), and the NTOWFv1 of the previous password (if it exists) for the machine account whose security identifier ([[MS-ADA3]](%5bMS-ADA3%5d.pdf#Section_4517e8353ee644d4bb95a94b6966bfb0) section 2.237) corresponds to the generated SID. If the machine account cannot be found, or the machine account does not correspond to a machine, or the machine account is disabled, the server MUST return ERROR\_NO\_SUCH\_USER. When the server is an [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) and the NTOWFv1 of the current password cannot be retrieved, the server MUST return ERROR\_NO\_TRUST\_LSA\_SECRET.

The digest of the *Message* parameter MUST be calculated with the following algorithm, using this [**one-way function (OWF)**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of the password.

1. CALL MD5Init(md5context)
2. IF OWF of password is present
3. CALL MD5Update(md5context, OWF of password, length of OWF of
4. password)
5. CALL MD5Update(md5context, Message, MessageSize)
6. CALL MD5Final(md5context)
7. SET digest to md5context.digest

The *NewMessageDigest* parameter MUST be computed by using the current password. The *OldMessageDigest* parameter MUST be computed by using the previous password, if it exists. If the previous password is not present, the new password MAY[<227>](#Appendix_A_227" \o "Product behavior note 227) be used to compute the *OldMessageDigest*.

Creating a message digest for the previous password allows the possibility of password replication latency to be accounted for. If the machine account password was recently changed, but the change has not propagated to the server processing this method, the server keeps the old password.

##### NetrLogonComputeClientDigest (Opnum 25)

The NetrLogonComputeClientDigest method is used by a client to compute a cryptographic digest of a message by using the MD5 message-digest algorithm, as specified in [[RFC1321]](https://go.microsoft.com/fwlink/?LinkId=90275). This method is called by a client to compute a message digest, as specified in this section. The client SHOULD[<228>](#Appendix_A_228" \o "Product behavior note 228) use this digest to compare against one that is returned by a call to [NetrLogonComputeServerDigest](#Section_5f95c374795142d9816cc7f4cff2ed52). This comparison allows the client to ensure that the server that it communicates with knows the [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) between the client machine and the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

1. NET\_API\_STATUS NetrLogonComputeClientDigest(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string, unique] wchar\_t\* DomainName,
4. [in, size\_is(MessageSize)] UCHAR \* Message,
5. [in] ULONG MessageSize,
6. [out] CHAR NewMessageDigest[16],
7. [out] CHAR OldMessageDigest[16]
8. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**DomainName:** A pointer to a null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) or [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain. If this parameter is NULL, the domain of which the client computer is a member is used.

**Message:** A pointer to a buffer that contains the message for which the digest is to be computed.

**MessageSize:** The length, in bytes, of the *Message* parameter.

**NewMessageDigest:** A 128-bit MD5 digest of the current computer account password and the message in the *Message* buffer.

**OldMessageDigest:** A 128-bit MD5 digest of the previous machine account password and the message in the *Message* buffer. If no previous computer account password exists, the current password is used.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

If the client does not have sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940), the server MUST return ERROR\_ACCESS\_DENIED.

The server MUST compute or retrieve the NTOWFv1 of the current machine password and the NTOWFv1 of the previous machine password, if it exists. If the password cannot be found, the server MUST return ERROR\_NO\_TRUST\_LSA\_SECRET.

The server MUST compute the NTOWFv1 (as specified in [[MS-NLMP]](%5bMS-NLMP%5d.pdf#Section_b38c36ed28044868a9ff8dd3182128e4) section 3.3.1) of each password, if present. The digest of the *Message* parameter MUST be calculated using this [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of the password, as follows.

1. CALL MD5Init(md5context)
2. IF OWF of password is present
3. CALL MD5Update(md5context, OWF of password, length of OWF of
4. password)
5. CALL MD5Update(md5context, Message, MessageSize)
6. CALL MD5Final(md5context)
7. SET digest to md5context.digest

The *NewMessageDigest* parameter MUST be computed by using the current password. The *OldMessageDigest* parameter MUST be computed by using the previous password, if it exists. If the previous password is not present, the new password MUST be used to compute the *OldMessageDigest*.

Creating a message digest for the previous password allows the possibility of password replication latency to be accounted for. If the client computer password was recently changed, but the change has not propagated to the server processing this method, the client and the server will have two different passwords.

##### NetrLogonSendToSam (Opnum 32)

The NetrLogonSendToSam method allows a BDC or [**RODC**](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870) to forward user account password changes to the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). It SHOULD[<229>](#Appendix_A_229" \o "Product behavior note 229) be used by the client to deliver an opaque buffer to the [**SAM database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b) ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 3.1.1) on the server side.

1. NTSTATUS NetrLogonSendToSam(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in, size\_is(OpaqueBufferSize)]
7. UCHAR \* OpaqueBuffer,
8. [in] ULONG OpaqueBufferSize
9. );

**PrimaryName:** The custom binding handle, as defined in [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**ComputerName:** A null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the [**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf) of the client computer making the call.

**Authenticator:** A pointer to a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure, as specified in section 2.2.1.1.5, that contains the client [**authenticator**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3).

**ReturnAuthenticator:** A pointer to a NETLOGON\_AUTHENTICATOR structure, as specified in section 2.2.1.1.5, that contains the server return authenticator.

**OpaqueBuffer:** A buffer to be passed to the [**Security Account Manager (SAM)**](#gt_0b53d5bb-74ab-4705-8657-c22d32781103) service on the PDC. The buffer is encrypted on the wire.

**OpaqueBufferSize:** The size, in bytes, of the *OpaqueBuffer* parameter.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* Apply Common Error Processing Rule A, specified in section [3](#Section_2d776bfce81f4c8f9da84c2920f65413).
* Using the *ComputerName* for the [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to find the corresponding record in the ClientSessionInfo table, verify the *Authenticator* parameter (section [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806)). If the *Authenticator* parameter is valid, compute the *ReturnAuthenticator* parameter returned (section 3.1.4.5). Otherwise, the server MUST return STATUS\_ACCESS\_DENIED.

If the *PrimaryName* parameter is not NULL, it is compared against the server's [**computer name**](#gt_9a7bc8b3-3374-4608-8f73-be20a90b898b). If the *PrimaryName* parameter does not match the server's computer name, the server MUST return STATUS\_INVALID\_COMPUTER\_NAME. If the *PrimaryName* parameter matches the server's computer name, or the *PrimaryName* parameter is NULL, then processing proceeds.

The server MUST check whether the caller is a BDC or RODC; otherwise, it MUST return STATUS\_ACCESS\_DENIED. The server determines whether the caller is BDC or RODC by examining the value of *SecureChannelType* parameter in the ClientSessionInfo table. The caller is a BDC if *SecureChannelType* is ServerSecureChannel. The caller is an RODC if the *SecureChannelType* is CdcServerSecureChannel.

The server MUST decrypt the message passed in the *OpaqueBuffer* parameter using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the **NegotiateFlags** member of the **ClientSessionInfo** table entry for *ComputerName*) and the established [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) as the [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) key. The server SHOULD pass the decrypted data to the local SAM for processing. The buffer specified by *OpaqueBuffer* is completely opaque to the Netlogon Protocol.

This method can be called only by a machine that has established a secure channel with the server.

##### NetrLogonSetServiceBits (Opnum 22)

The NetrLogonSetServiceBits method SHOULD[<230>](#Appendix_A_230" \o "Product behavior note 230) be used to notify Netlogon whether a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) is running specified services, as detailed in the following section.

1. NTSTATUS NetrLogonSetServiceBits(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] DWORD ServiceBitsOfInterest,
4. [in] DWORD ServiceBits
5. );

**ServerName:** The custom binding handle, as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640), representing the connection to a DC.

**ServiceBitsOfInterest:** A set of bit flags used as a mask to indicate which service's state (running or not running) is being set by this call. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | 0 | 0 | 0 | B | 0 | 0 | A | 0 | 0 | 0 | 0 | 0 | 0 |

The flags SHOULD[<231>](#Appendix_A_231" \o "Product behavior note 231) be defined as follows.

| Value | Description |
| --- | --- |
| A | The state of the time service is being set. |
| B | The state of the time service with clock hardware is being set. |
| C | The state of the Active Directory Web service is being set. |

All other bits MUST be set to zero; otherwise, the error STATUS\_ACCESS\_DENIED is returned.

**ServiceBits:** A set of bit flags used as a mask to indicate whether the service indicated by *ServiceBitsOfInterest* is running. If the flag is set to 0, the corresponding service indicated by *ServiceBitsOfInterest* is not running. Otherwise, if the flag is set to 1, the corresponding service indicated by *ServiceBitsOfInterest* is running. The value is constructed from zero or more bit flags from the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 1  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 2  0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 3  0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C | 0 | 0 | 0 | B | 0 | 0 | A | 0 | 0 | 0 | 0 | 0 | 0 |

The flags SHOULD[<232>](#Appendix_A_232" \o "Product behavior note 232) be defined as follows.

| Value | Description |
| --- | --- |
| A | Time service is running. |
| B | Time service with clock hardware is running. |
| C | Active Directory Web service is running. |

All other bits MUST be set to zero; otherwise, the error STATUS\_INVALID\_PARAMETER is returned.

If a flag is set to 1 and the same flag is set to 0 in the *ServiceBitsOfInterest* parameter, the error STATUS\_INVALID\_PARAMETER is returned.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The server SHOULD[<233>](#Appendix_A_233" \o "Product behavior note 233) return ERROR\_ACCESS DENIED if the caller is not local.

If the client does not have sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940), the server MUST return ERROR\_ACCESS\_DENIED.

The server MUST return STATUS\_ACCESS\_DENIED if bits other than those previously specified are passed in.

For every service state being set by this call, as indicated by *ServiceBitsOfInterest*, the state of the corresponding service ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.1.2), as indicated by *ServiceBits*, is updated in the **ServerServiceBits** ADM element.

##### NetrLogonGetTimeServiceParentDomain (Opnum 35)

The NetrLogonGetTimeServiceParentDomain method SHOULD[<234>](#Appendix_A_234" \o "Product behavior note 234) return the name of the parent [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) of the current domain. The [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) returned by this method is suitable for passing into the [NetrLogonGetTrustRid](#Section_1d6fad9e763d495f9bed18c79304c3d7) method and [NetrLogonComputeClientDigest](#Section_79ca6e90ccd2429eb5ac8050b620eef6) method.

1. NET\_API\_STATUS NetrLogonGetTimeServiceParentDomain(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [out, string] wchar\_t\*\* DomainName,
4. [out] int\* PdcSameSite
5. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**DomainName:** A pointer to the buffer that receives the null-terminated [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8) string that contains the name of the parent domain. If the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) domain name is available, it is returned through this parameter; otherwise, the NetBIOS domain name is returned.

**PdcSameSite:** A pointer to the integer that receives the value that indicates whether the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) for the domain *DomainName* is in the same [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba) as the server specified by *ServerName*. This value SHOULD[<235>](#Appendix_A_235" \o "Product behavior note 235) be ignored if *ServerName* is not a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd).

| Value | Meaning |
| --- | --- |
| False  0 | The PDC is not in the same site as the server specified by *ServerName*. |
| True  1 | The PDC is in the same site as the server specified by *ServerName*. |

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

The server SHOULD[<236>](#Appendix_A_236" \o "Product behavior note 236) return ERROR\_ACCESS DENIED if the caller is not local.

If the client does not have sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940), the server MUST return ERROR\_ACCESS\_DENIED.

The domain name returned MUST be determined according to the following rules:

* On a non-DC machine, the returned domain name is the name of the domain of which the *ServerName* is a member. If *ServerName* is not valid, the server MUST return ERROR\_INVALID\_COMPUTERNAME.
* On a DC that is at the root of the [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62), **rootDomainNamingContext** ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 3.1.1.3.2.16) is equal to **defaultNamingContext** ([MS-ADTS] section 3.1.1.3.2.3). In this case, ERROR\_NO\_SUCH\_DOMAIN is returned.
* On a DC that is at the root of a [**domain tree**](#gt_e2c071f1-5977-4749-868f-6c5a04929476) in the forest, the name of a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain that is also at the root of a domain tree in the forest is returned.

On any other DC, the name of the domain that is directly the parent domain is returned.

The domain's information MUST be retrieved from an implementation-specific directory. Based on this retrieved information, if the domain has a DNS domain name, it MUST be returned; otherwise, the NetBIOS domain name MUST be returned. This behavior is functionally equivalent to locally invoking LsarQueryTrustedDomainInfo ([[MS-LSAD]](%5bMS-LSAD%5d.pdf#Section_1b5471ef4c334a91b079dfcbb82f05cc) section 3.1.4.7.2) for the domain, where TrustedDomainSid is the domain [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) corresponding to the appropriate domain name retrieved from a cached list, and InformationClass is TrustedDomainInformationEx (policy handle is not needed locally), to return the TrustedDomainInformationEx.Name string (DNS name) if it is present or TrustedDomainInformationEx.Flat Name string ([**NetBIOS name**](#gt_0334e0bd-2755-42f6-aeff-2d4a22bf4abf)) otherwise.

The *PdcSameSite* returned MUST be determined according to the following rules:

* On a non-DC machine, the value of *PdcSameSite* is set to TRUE.
* On a DC machine, the server SHOULD determine the PDC as specified in [MS-ADTS] section 3.1.1.1.11. Then the server SHOULD determine the sites of both the server and PDC as described in [MS-ADTS] section 3.1.1.4.5.29. The server MUST compare the PDC site with its own site, and if the two match, the *PdcSameSite* output parameter MUST be set to TRUE; otherwise, it MUST be set to FALSE.

#### Administrative Services Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) are used for querying and controlling Netlogon behavior, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7).

##### NetrLogonControl2Ex (Opnum 18)

The NetrLogonControl2Ex method SHOULD[<237>](#Appendix_A_237" \o "Product behavior note 237) execute administrative actions that pertain to the Netlogon server operation. It is used to query the status and control the actions of the Netlogon server.

1. NET\_API\_STATUS NetrLogonControl2Ex(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] DWORD FunctionCode,
4. [in] DWORD QueryLevel,
5. [in, switch\_is(FunctionCode)] PNETLOGON\_CONTROL\_DATA\_INFORMATION Data,
6. [out, switch\_is(QueryLevel)] PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
7. );

**ServerName:** The custom [**binding handle**](#gt_44deb72d-c62b-4335-90e4-b9fd4dd782ed), as defined in section [3.5.4.1](#Section_3b224201b53143e28c79b61f6dea8640).

**FunctionCode:** The control operation to be performed; it SHOULD[<238>](#Appendix_A_238" \o "Product behavior note 238) be one of the following values:

| Value | Meaning |
| --- | --- |
| NETLOGON\_CONTROL\_QUERY  0x00000001 | No operation; only the requested information is returned. |
| NETLOGON\_CONTROL\_REPLICATE  0x00000002 | Forces a BDC to perform an immediate partial synchronization of all [**databases**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15), as detailed in section [3.6.5.2.2](#Section_870c890e74fc4850aa8b5599299e390a).[<239>](#Appendix_A_239" \o "Product behavior note 239) |
| NETLOGON\_CONTROL\_SYNCHRONIZE  0x00000003 | Forces a BDC to perform an immediate full synchronization of all databases.[<240>](#Appendix_A_240" \o "Product behavior note 240) |
| NETLOGON\_CONTROL\_PDC\_REPLICATE  0x00000004 | Forces a [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to immediately send announcement messages to ask each BDC to replicate the database for details (see section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761)). |
| NETLOGON\_CONTROL\_REDISCOVER  0x00000005 | Forces the server to rediscover a [**domain controller**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the specified [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) and to set up a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) to the discovered DC. |
| NETLOGON\_CONTROL\_TC\_QUERY  0x00000006 | Queries the status of the last usage of the secure channel to the DC. |
| NETLOGON\_CONTROL\_TRANSPORT\_NOTIFY  0x00000007 | Notifies the Netlogon server that a new network connection has been added, and causes the server to flush any DC cache. |
| NETLOGON\_CONTROL\_FIND\_USER  0x00000008 | Queries the name of a [**trusted**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) domain that contains an account for a user. |
| NETLOGON\_CONTROL\_CHANGE\_PASSWORD  0x00000009 | Causes the server to generate a new [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) and to set it on the account used by the DC for setting up the secure channel from the server. |
| NETLOGON\_CONTROL\_TC\_VERIFY  0x0000000A | Verifies the current status of the server's secure channel to a DC in the specified domain. |
| NETLOGON\_CONTROL\_FORCE\_DNS\_REG  0x0000000B | Triggers the non-timer event, Force Register DNS Records, described in [[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.3.2.2.1. |
| NETLOGON\_CONTROL\_QUERY\_DNS\_REG  0x0000000C | SHOULD[<241>](#Appendix_A_241" \o "Product behavior note 241) query the status of [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) updates performed by the Netlogon server, as described in [MS-ADTS] section 6.3.2. |
| NETLOGON\_CONTROL\_BACKUP\_CHANGE\_LOG  0x0000FFFC | Used for debugging purposes and does not affect the Netlogon protocol behavior.[<242>](#Appendix_A_242" \o "Product behavior note 242) |
| NETLOGON\_CONTROL\_TRUNCATE\_LOG  0x0000FFFD | Used for debugging purposes and does not affect the Netlogon protocol behavior.[<243>](#Appendix_A_243" \o "Product behavior note 243) |
| NETLOGON\_CONTROL\_SET\_DBFLAG  0x0000FFFE | Used for debugging purposes and does not affect the Netlogon protocol behavior.[<244>](#Appendix_A_244" \o "Product behavior note 244) |
| NETLOGON\_CONTROL\_BREAKPOINT  0x0000FFFF | Used for debugging purposes and MUST be used only with [**checked builds**](#gt_cd33ef8c-8d58-43b6-9273-fa308fc1caf1).[<245>](#Appendix_A_245" \o "Product behavior note 245) Calling NetrLogonControl2Ex with this function code does not affect the Netlogon protocol behavior.[<246>](#Appendix_A_246" \o "Product behavior note 246) |

**QueryLevel:** Information query level requested by the client. The buffer returned in the *Buffer* parameter contains one of the following structures, based on the value of this field.

| Value | Buffer Contents |
| --- | --- |
| 0x00000001 | A [NETLOGON\_INFO\_1](#Section_afeb873c48264beba35cae73a708b108) structure is returned. |
| 0x00000002 | A [NETLOGON\_INFO\_2](#Section_c48a87004c174afb8866f0cfc0c0a671) structure is returned. |
| 0x00000003 | A [NETLOGON\_INFO\_3](#Section_be92a2cd950c4b268cd3475065406b92) structure is returned. |
| 0x00000004 | A [NETLOGON\_INFO\_4](#Section_a2b4c31118314de6bf5efe8427323144) structure is returned.[<247>](#Appendix_A_247" \o "Product behavior note 247) |

**Data:** A [NETLOGON\_CONTROL\_DATA\_INFORMATION](#Section_ab0e203d5f69469c8c577b6a0b1308b9) structure, as specified in section 2.2.1.7.1, that contains specific data required by the query.

**Buffer:** A [NETLOGON\_CONTROL\_QUERY\_INFORMATION](#Section_c5d2469cf0c347de87950e22f1070337) structure, as specified in section 2.2.1.7.6, that contains the specific query results, with a level of verbosity as specified in *QueryLevel*.

**Return Values:** The method returns 0x00000000 on success; otherwise, it returns a nonzero error code.

On receiving this call, the server MUST perform the following validation steps:

* The server uses the server name passed in the *ServerName* parameter to look up the domain for the request. If the name is not found, the server MUST return ERROR\_INVALID\_COMPUTERNAME.
* If the client does not have sufficient [**privilege**](#gt_d8092e10-b227-4b44-b015-511bb8178940), the server MUST return ERROR\_ACCESS\_DENIED.
* The *QueryLevel* parameter MUST contain a value between 1 and 4; otherwise, the server MUST return ERROR\_INVALID\_LEVEL.
  + When the *QueryLevel* parameter is set to 0x00000004, the *FunctionCode* parameter MUST be set to NETLOGON\_CONTROL\_FIND\_USER (0x00000008); otherwise, the server MUST return ERROR\_INVALID\_PARAMETER.
  + When the *QueryLevel* parameter is set to 0x00000002, the *FunctionCode* parameter MUST be set to NETLOGON\_CONTROL\_REDISCOVER (0x00000005), NETLOGON\_CONTROL\_TC\_QUERY (0x00000006), or NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A); otherwise, the server MUST return ERROR\_INVALID\_PARAMETER.
* When the *FunctionCode* parameter is set to:
  + NETLOGON\_CONTROL\_FIND\_USER (0x00000008), the *QueryLevel* parameter MUST be set to 0x00000004; otherwise, the server MUST return ERROR\_INVALID\_PARAMETER.
  + NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A), the *QueryLevel* parameter MUST be set to 0x00000002; otherwise, the server MUST return ERROR\_INVALID\_PARAMETER.
  + NETLOGON\_CONTROL\_QUERY\_DNS\_REG (0x0000000C), the *QueryLevel* parameter MUST be set to 0x00000001; otherwise, the server MUST return ERROR\_INVALID\_LEVEL.
* The server MUST verify the *Data* parameter for the NETLOGON\_CONTROL\_REDISCOVER (0x00000005), NETLOGON\_CONTROL\_TC\_QUERY (0x00000006), NETLOGON\_CONTROL\_FIND\_USER (0x00000008), NETLOGON\_CONTROL\_CHANGE\_PASSWORD (0x00000009), and NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A) function codes:
  + If the parameter is NULL, the server MUST return ERROR\_INVALID\_PARAMETER.
  + For the NETLOGON\_CONTROL\_REDISCOVER (0x00000005), NETLOGON\_CONTROL\_TC\_QUERY (0x00000006), NETLOGON\_CONTROL\_CHANGE\_PASSWORD (0x00000009), and NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A) function codes, if the parameter does not contain a valid [**domain name**](#gt_45a1c9f1-0263-49a8-97c7-7aca1a99308c) in the trust list, the server MUST return ERROR\_NO\_SUCH\_DOMAIN.
  + For the NETLOGON\_CONTROL\_FIND\_USER (0x00000008) function code, if the parameter does not contain a valid user name, the server MUST return NERR\_UserNotFound.

For other function codes, the *Data* parameter is ignored.

Based on the *FunctionCode* parameter provided by the client, the server MUST complete the following before populating the return structure:

* NETLOGON\_CONTROL\_QUERY: Nothing.
* NETLOGON\_CONTROL\_REPLICATE: Return ERROR\_NOT\_SUPPORTED.[<248>](#Appendix_A_248" \o "Product behavior note 248)
* NETLOGON\_CONTROL\_SYNCHRONIZE: Return ERROR\_NOT\_SUPPORTED.[<249>](#Appendix_A_249" \o "Product behavior note 249)
* NETLOGON\_CONTROL\_PDC\_REPLICATE: Return ERROR\_NOT\_SUPPORTED.[<250>](#Appendix_A_250" \o "Product behavior note 250)
* NETLOGON\_CONTROL\_REDISCOVER: Force the server to rediscover DCs in the domain name provided in the **TrustedDomainName** field of the *Data* parameter and to set up a secure channel (section [3.1](#Section_273b6905782d4a7ea2e44337816916e0)) to the discovered DC. DC rediscovery is the same as initial DC discovery (section [3.1.4.10](#Section_00ac739d274d434b9efbfad10405721a)). If a DC discovery and establishment of a secure channel to the DC fails, the error ERROR\_NO\_LOGON\_SERVERS is returned.
* NETLOGON\_CONTROL\_TC\_QUERY: Provide return data based on the DC in the domain name provided in the **TrustedDomainName** field of the *Data* parameter.
* NETLOGON\_CONTROL\_TRANSPORT\_NOTIFY: In order to allow the server to immediately retry establishing a secure session over the new network connection that became available, the server SHOULD set the **LastAuthenticationTry** member of every entry in the ServerSession table maintained by the Netlogon client on the server's machine to zero, enumerating across every entry in the table. Also, if the server has a DC cache, the server SHOULD flush the **LocatedDCsCache** and **FailedDiscoveryCache**.
* NETLOGON\_CONTROL\_FIND\_USER: Query the name of a trusted domain that contains an account for a user with the user name provided in the **UserName** field of the *Data* parameter. The server MUST be a DC; otherwise, return ERROR\_NOT\_SUPPORTED.
* NETLOGON\_CONTROL\_CHANGE\_PASSWORD: Generate a new shared secret for the domain name provided in the **TrustedDomainName** field of the *Data* parameter. The server MUST update the **SharedSecret** (section [3.1.1](#Section_708b71329e72447c992bd0bef4078f81)). If the **TrustedDomainName** field of the *Data* parameter is a trust name and the server is not a PDC ([MS-ADTS] section 6.1.5.3), the server MUST return ERROR\_INVALID\_DOMAIN\_ROLE.
* NETLOGON\_CONTROL\_TC\_VERIFY: Call any Netlogon method that requires a secure channel (section [3.1.4.6](#Section_f61c3f4a53ff4f3090066d93a2162ef8)) to the DCC in the domain name provided in the **TrustedDomainName** field of the *Data* parameter.
* NETLOGON\_CONTROL\_FORCE\_DNS\_REG: The DC SHOULD re-register all of its DNS records ([MS-ADTS] section 6.3.2).[<251>](#Appendix_A_251" \o "Product behavior note 251)
* NETLOGON\_CONTROL\_QUERY\_DNS\_REG: Query the status of DNS updates performed by the Netlogon server.[<252>](#Appendix_A_252" \o "Product behavior note 252)
* NETLOGON\_CONTROL\_BACKUP\_CHANGE\_LOG: Nothing.
* NETLOGON\_CONTROL\_TRUNCATE\_LOG: Nothing.
* NETLOGON\_CONTROL\_SET\_DBFLAG: Nothing.
* NETLOGON\_CONTROL\_BREAKPOINT: Nothing.

The following describes the output generated in the *Buffer* parameter based on the *FunctionCode* and *QueryLevel* requested.

For *QueryLevel* 1, the return structure MUST be generated as follows:

* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo1.netlog1\_flags** MUST be set to the **netlog1\_flags** values that are applicable to the server. See NETLOGON\_INFO\_1 (section 2.2.1.7.2) for a description of the netlog1\_flags field.
* If the *FunctionCode* parameter has the value NETLOGON\_CONTROL\_QUERY\_DNS\_REG (0x0000000C), and any DNS registration or deregistration ([MS-ADTS] section 6.3.2) errors occurred on the last completed update, then the NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo1.netlog1\_flags G bit MUST be set. Otherwise, the NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo1.netlog1\_flags G bit MUST NOT be set.
* If this is a non-PDC computer, **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo1.netlog1\_pdc\_connection\_status** MUST be set to the current connection status of the PDC, which is stored in the **ConnectionStatus** field of the **ServerSessionInfo** table. This field MUST be set to zero if this server is the PDC.
* If *FunctionCode* NETLOGON\_CONTROL\_PDC\_REPLICATE (0x00000004) is supported and **ntMixedDomain** is set to zero, the server MUST return ERROR\_NOT\_SUPPORTED. Otherwise, the server SHOULD return ERROR\_SUCCESS.

For *QueryLevel* 2, the return structure MUST be generated as follows:

* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_flags** MUST be set to the **netlog2\_flags** values that are applicable to the server. For a description of the **netlog2\_flags** member, see 2.2.1.7.3.
* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set as follows.
* Call NetrServerGetTrustInof to the DC with which it has an established secure channel for the domain specified in the *Data.TrustedDomainName* parameter received.
* If the server returns STATUS\_NOT\_SUPPORTED, then NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status MUST be set to the value of the ConnectionStatus field from the ServerSessionInfo table.
  + - If the server returns anything else and ServerSessionInfo.ConnectionStatus is not STATUS\_SUCCESS, then **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set to the value of **ConnectionStatus** field from the **ServerSessionInfo** table.
    - Otherwise, the **ConnectionStatus** field of the **ServerSessionInfo** table is STATUS\_SUCCESS and the following rules apply:
      1. If the *TrustInfo* value returned by NetrServerGetTrustInfo is not NULL and the *ULongEntryCount* value is greater than 0, then process the first ULONG element in the *UlongData* array as follows:
         * If the TRUST\_ATTRIBUTE\_FOREST\_TRANSITIVE (0x00000008) bit is set, and if the server processing the element is either of the following:

Workstation: **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set to STATUS\_DOMAIN\_TRUST\_INCONSISTENT.

Domain controller (DC): If the D flag is not set in the TrustedDomains.TrustAttributes for the domain specified in the *Data.TrustedDomainName* parameter received, then **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set to STATUS\_DOMAIN\_TRUST\_INCONSISTENT.

* + - * + Otherwise, if the server processing the element is a domain controller (DC) and the D flag is set in the TrustedDomains.TrustAttributes for the domain specified in the *Data.TrustedDomainName* parameter received, then **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set to STATUS\_DOMAIN\_TRUST\_INCONSISTENT.
      1. Verify that the SharedSecret stored locally is the same as what was returned by NetrServerGetTrustInfo in EncryptedNewOwfPassword and EncryptedOldOwfPassword. If the SecureChannelType returned by NetrServerGetTrustInfo is **TrustedDnsDomainSecureChannel** or **TrustedDomainSecureChannel**, then verify using the local trust secrets. For all other types of *SecureChannelType* values, verify using the **SharedSecret** of the computer account. If verification fails, then **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** MUST be set to STATUS\_WRONG\_PASSWORD.
      2. If **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_pdc\_connection\_status** has not been set, then it MUST be set to STATUS\_SUCCESS.
* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_trusted\_dc\_name** MUST be set to the name of the DC with which the computer has a secure channel established, which is stored in the **DCName** field of the **ServerSessionInfo** table.
* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo2.netlog2\_tc\_connection\_status** MUST be set to the status of the secure channel, which is stored in the ConnectionStatus field of the ServerSessionInfo table.

For *QueryLevel* 3, the return structure MUST be generated as follows:

* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo3.netlog3\_flags** MUST be set to zero.
* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo3.netlog3\_logon\_attempts** MUST be set to LogonAttempts.
* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo3.netlog3\_reserved1** through **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo3.netlog3\_reserved5** MUST be set to zero.

For *QueryLevel* 4, the return structure MUST be generated as follows:

* **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo4.netlog4\_trusted\_domain\_name** MUST be set to the trusted domain that the user was found in. **NETLOGON\_CONTROL\_QUERY\_INFORMATION.NetlogonInfo4.netlog4\_trusted\_dc\_name** MUST be set to the DC in the trusted domain.

In addition, the returned *Buffer* structure contains undefined data of varied size at the end, which MUST be ignored.

##### NetrLogonControl2 (Opnum 14)

The NetrLogonControl2 method[<253>](#Appendix_A_253" \o "Product behavior note 253) is a predecessor to the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method (section 3.5.4.9.1) and is updated to have the same functionality as NetrLogonControl2Ex. All parameters of this method have the same meanings as the identically named parameters of the NetrLogonControl2Ex method.

1. NET\_API\_STATUS NetrLogonControl2(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] DWORD FunctionCode,
4. [in] DWORD QueryLevel,
5. [in, switch\_is(FunctionCode)] PNETLOGON\_CONTROL\_DATA\_INFORMATION Data,
6. [out, switch\_is(QueryLevel)] PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
7. );

All restrictions on parameter values in the NetrLoginControl2Ex method (section 3.5.4.9.1) apply. Extra restrictions are applied to the values of the *QueryLevel* parameter as follows:

* If the *QueryLevel* parameter is set to 0x00000004, the error ERROR\_INVALID\_LEVEL is returned.

Message processing is identical to NetrLogonControl2Ex (section 3.5.4.9.1).

##### NetrLogonControl (Opnum 12)

The NetrLogonControl method is a predecessor to the [NetrLogonControl2Ex](#Section_650a105f64434eb0839a188708328fb0) method (section [3.5.4.9.1](#Section_df7e5dd1ebcc47549da02e0bded82d29)). All parameters of this method SHOULD[<254>](#Appendix_A_254" \o "Product behavior note 254) have the same meanings as the identically named parameters of the NetrLogonControl2Ex method.

1. NET\_API\_STATUS NetrLogonControl(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in] DWORD FunctionCode,
4. [in] DWORD QueryLevel,
5. [out, switch\_is(QueryLevel)] PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
6. );

All restrictions on parameter values in the NetrLogonControl2Ex method (section 3.5.4.9.1) apply. Extra restrictions are applied to the values of the *FunctionCode*[<255>](#Appendix_A_255" \o "Product behavior note 255) and *QueryLevel* parameters as follows:

* The value of *QueryLevel* parameter is restricted to 0x00000001. If 0x00000002 is used, the error ERROR\_NOT\_SUPPORTED is returned; if any value larger than 0x00000002 is used, the error ERROR\_INVALID\_LEVEL is returned.

Message processing is identical to NetrLogonControl2Ex (section 3.5.4.9.1), except for the following:

* The *Data* parameter of **NetrLogonControl2Ex** is set to NULL.

#### Obsolete Methods

Methods in this [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac) support LAN Manager products and are now obsolete, as outlined in section [1.3](#Section_70d9e96a9e32432188334b597efc87a7). They SHOULD[<256>](#Appendix_A_256" \o "Product behavior note 256) be rejected with an error code.

##### NetrLogonUasLogon (Opnum 0)

1. NET\_API\_STATUS NetrLogonUasLogon(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string] wchar\_t\* UserName,
4. [in, string] wchar\_t\* Workstation,
5. [out] PNETLOGON\_VALIDATION\_UAS\_INFO\* ValidationInformation
6. );

##### NetrLogonUasLogoff (Opnum 1)

1. NET\_API\_STATUS NetrLogonUasLogoff(
2. [in, unique, string] LOGONSRV\_HANDLE ServerName,
3. [in, string] wchar\_t\* UserName,
4. [in, string] wchar\_t\* Workstation,
5. [out] PNETLOGON\_LOGOFF\_UAS\_INFO LogoffInformation
6. );

##### NetrAccountDeltas (Opnum 9)

1. NTSTATUS NetrAccountDeltas(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] PUAS\_INFO\_0 RecordId,
7. [in] DWORD Count,
8. [in] DWORD Level,
9. [out, size\_is(BufferSize)] UCHAR \* Buffer,
10. [in] DWORD BufferSize,
11. [out] ULONG \* CountReturned,
12. [out] ULONG \* TotalEntries,
13. [out] PUAS\_INFO\_0 NextRecordId
14. );

##### NetrAccountSync (Opnum 10)

1. NTSTATUS NetrAccountSync(
2. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
3. [in, string] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD Reference,
7. [in] DWORD Level,
8. [out, size\_is(BufferSize)] UCHAR \* Buffer,
9. [in] DWORD BufferSize,
10. [out] ULONG \* CountReturned,
11. [out] ULONG \* TotalEntries,
12. [out] ULONG \* NextReference,
13. [out] PUAS\_INFO\_0 LastRecordId
14. );

### Timer Events

None.

### Other Local Events

When Netlogon receives a PolicyChange event ([[MS-GPOD]](%5bMS-GPOD%5d.pdf#Section_6e6349392ccf4412b75f0035dc05ea67) section 2.8.2), NRPC implementations SHOULD[<257>](#Appendix_A_257" \o "Product behavior note 257) load the new value.

## Netlogon NT Replication Details

Netlogon replication is a single master replication in which the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) serves as the replication master. [<258>](#Appendix_A_258" \o "Product behavior note 258) The PDC maintains a state for each BDC that includes the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) of the BDC [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). The PDC periodically sends announcement messages to BDCs with out-of-sync database serial numbers to notify them about database changes accumulated during the period. In response, BDCs receiving the message update their database by making synchronization calls to the PDC using [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331). The PDC updates the database serial number in the local state information for the BDC after processing the synchronization call from that BDC.

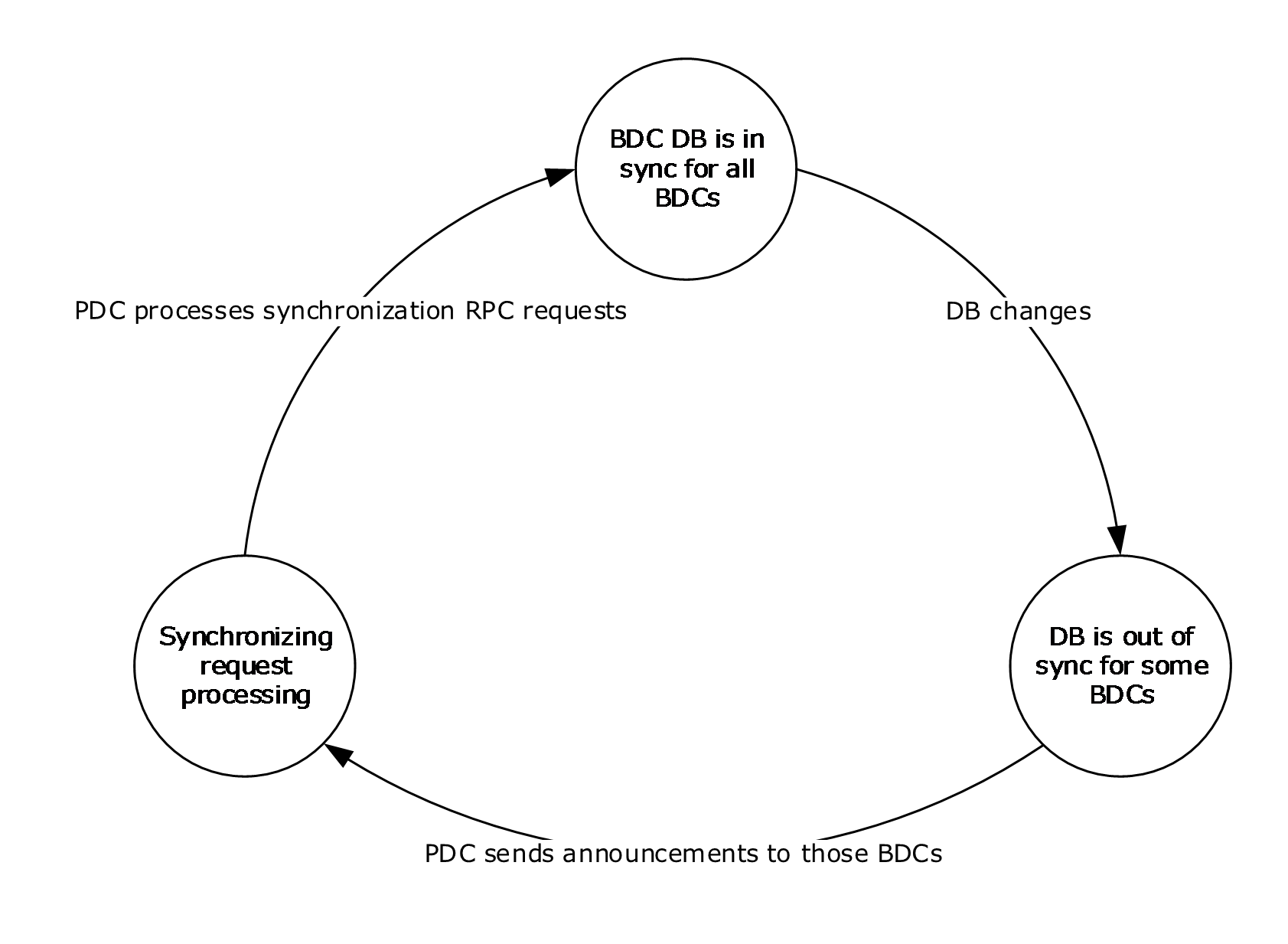


Figure 8: PDC States

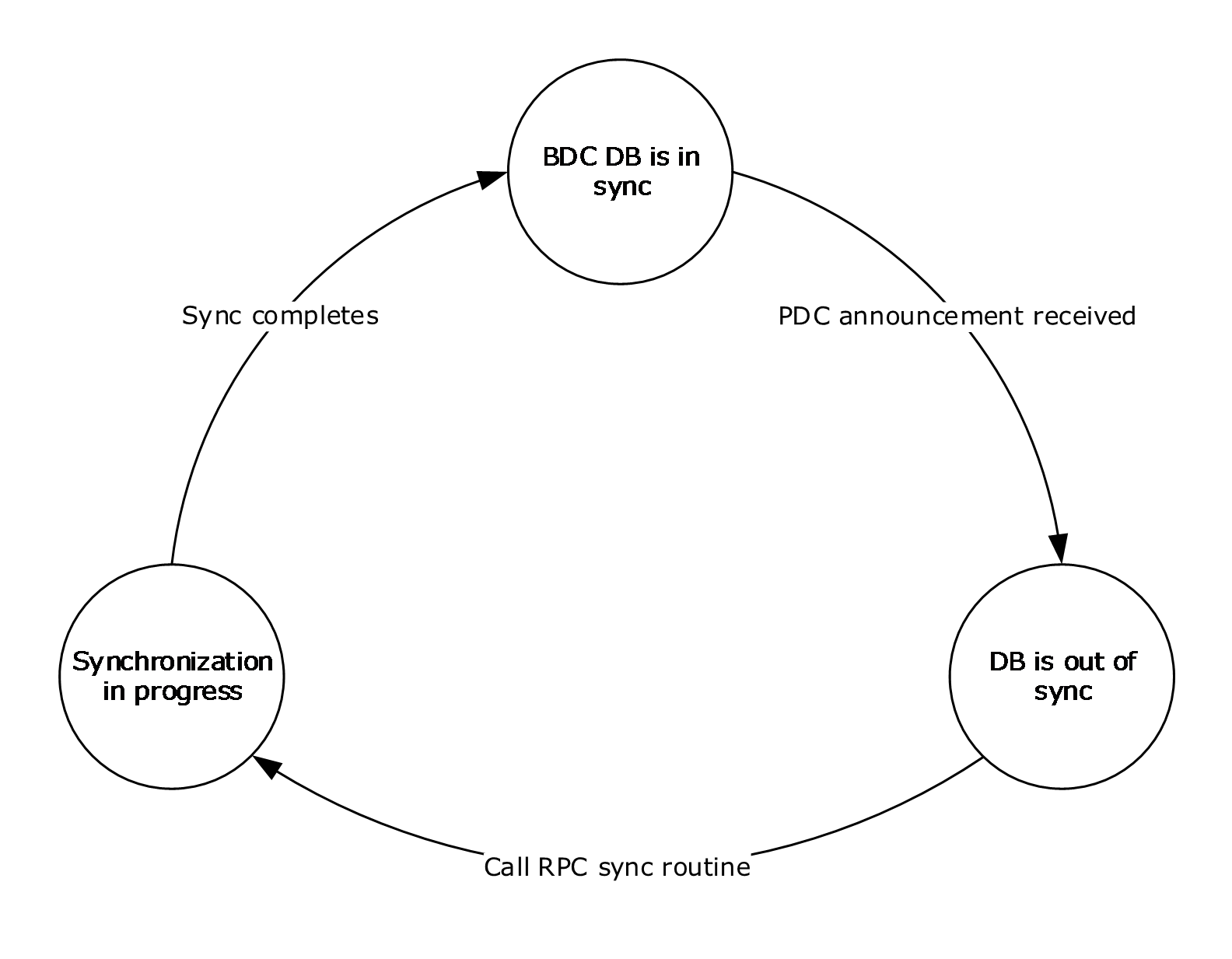


Figure 9: BDC States

### Abstract Data Model

The following section describes data organization and state maintained for purposes of Netlogon replication. The described organization is provided to explain how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

Each [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) maintains the following set of data.

**AbstractDomainName:** The name of the domain.

**AbstractDomainSid:** The [**SID**](#gt_83f2020d-0804-4840-a5ac-e06439d50f8d) of the domain.

**AbstractPrimaryDCName:** The name of the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d).

**AbstractBuiltinDatabaseCreationTime:** The QWORD time stamp in UTC for the [**SAM built-in database**](#gt_6bb6ffcf-2a22-4989-89ef-6c9937f91b8b) creation time.

**AbstractBuiltinDatabaseSerialNumber:** The [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) serial number of the SAM built-in database.

**AbstractSamDatabaseCreationTime:** The QWORD time stamp in UTC for the **SAM database** creation time.

**AbstractSamDatabaseSerialNumber:** The [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) of the SAM database.

**AbstractLsaDatabaseCreationTime:** The QWORD time stamp in UTC for the [**LSA database**](#gt_48a53a9a-6c9a-4df8-9882-1eccdf32340b) creation time.

**AbstractLsaDatabaseSerialNumber:** The database serial number of the LSA database.

Additionally, the PDC maintains the following set of data.

**AbstractPulse:** A setting on the PDC that specifies the period, in seconds, at which the announcement message will be sent periodically by the PDC to BDCs needing synchronization in the domain.

**AbstractRandom:** A setting on the PDC that indicates the amount of time, in seconds, that the BDC recipient of the message waits before contacting the PDC with a synchronization request.

**AbstractPulseConcurrency:** A setting on the PDC indicating the number of outstanding messages the PDC has sent to BDCs that haven't yet contacted the PDC with a synchronization request.

**AbstractMaximumPulse:** A setting on the PDC indicating a timeout value. If the last announcement message sent to a BDC was more than this value ago, the PDC will send a message to that BDC, as specified below.

**AbstractBdcDatabaseSerialNumbers:** An array of numbers that the PDC maintains to track database serial numbers for corresponding databases on BDCs.

Additionally, the BDC maintains the following set of data.

**AbstractFullSamSynchronizationNeeded:** A Boolean setting on the BDC that indicates whether full synchronization of the **SAM database** is needed. If TRUE, the BDC needs to perform full synchronization. If FALSE, the BDC needs to perform partial synchronization.

**AbstractFullBuiltinSynchronizationNeeded:** A Boolean setting on the BDC that indicates whether full synchronization of the SAM built-in database is needed. If TRUE, the BDC needs to perform full synchronization. If FALSE, the BDC needs to perform partial synchronization.

**AbstractFullLsaSynchronizationNeeded:** A Boolean setting on the BDC that indicates whether full synchronization of the LSA database is needed. If TRUE, the BDC needs to perform full synchronization. If FALSE, the BDC needs to perform partial synchronization.

### Timers

A timer is maintained on [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) to periodically notify BDCs of the changes to the [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) state. The protocol does not mandate a particular time-out value for the timer. The time-out can be configured between 1 minute and 2 days, inclusive. The default time-out is 5 minutes.

A timer is maintained on the BDC to start synchronization requests with the expiration time as described in section [3.6.3](#Section_b3773acfb5aa488c93550ad61767e4f2).

### Initialization

The [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) MUST register the [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) [**endpoint**](#gt_b91c1e27-e8e0-499b-8c65-738006af72ee). The PDC timer MUST be initialized to expire in AbstractPulse seconds. BDCs MUST create the \MAILSLOT\NET\NETLOGON [**mailslot**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78), as specified in section [2.1](#Section_592edbc8f6f140c09ab3fe6725ac6d7e). BDCs MUST initialize their BDC timers to never expire.

### Message Processing Events and Sequencing Rules

#### Message Processing on PDC

After the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) protocol initialization, the PDC MUST prepare an initial announcement message as follows:

* Set **LowSerialNumber** to the low DWORD part of AbstractSamDatabaseSerialNumber.
* Set **DateAndTime** to the value of AbstractSamDatabaseCreationTime expressed as the number of seconds elapsed since midnight of January 1, 1970.
* Set **Pulse** to the value of AbstractPulse.
* Set **Random** to the value of AbstractRandom.
* Set **PrimaryDCName** to the value of AbstractPrimaryDCName encoded in the [**OEM character set**](#gt_3240e34e-920e-40ac-a672-342ac34a5e22).
* Set **DomainName** to the value of AbstractDomainName encoded in the OEM character set.
* Optionally set **Pad** to 0x00 to make the next field in the message 2-byte aligned.
* Set **UnicodePrimaryDCName** to the value of AbstractPrimaryDCName encoded in [**Unicode**](#gt_c305d0ab-8b94-461a-bd76-13b40cb8c4d8).
* Set **UnicodeDomainName** to the value of AbstractDomainName encoded in Unicode.
* Set **DBCount** to 0x3.
* Set three **DBChangeInfo** fields as follows:
  + Set **DBIndex** of the 1st **DBChangeInfo** field to 0x0.

Set **LargeSerialNumber** of the 1st DBChangeInfo field to the value of AbstractSamDatabaseSerialNumber.

Set **DateAndTime** of the 1st **DBChangeInfo** field to the value of AbstractSamDatabaseCreationTime.

* + Set **DBIndex** of the 2nd **DBChangeInfo** field to 0x1.

Set **LargeSerialNumber** of the 2nd **DBChangeInfo** field to the value of AbstractBuiltinDatabaseSerialNumber.

Set **DateAndTime** of the 2nd **DBChangeInfo** field to the value of AbstractBuiltinDatabaseCreationTime.

* + Set **DBIndex** of the 3rd **DBChangeInfo** field to 0x2.

Set **LargeSerialNumber** of the 3rd **DBChangeInfo** field to the value of AbstractLsaDatabaseSerialNumber.

Set **DateAndTime** of the 3rd **DBChangeInfo** field to the value of AbstractLsaDatabaseCreationTime.

* Set **DBCount** to 0x3.
* Set **DomainSidSize** to the size in bytes of AbstractDomainSid.
* Set **DomainSid** to the value of AbstractDomainSid.

The PDC MUST send the message to all BDCs configured in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). In response to this message, the PDC MUST expect BDCs to synchronize their [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) by calling [NetrDatabaseSync](#Section_86683ada19a2414eafaf124f77dc4685), [NetrDatabaseSync2](#Section_31fc80bd4f4d4512a792e488bb78f6a0), or [NetrDatabaseDeltas](#Section_5412f0bc5eb94197b4c4c5a8c06ba018), as described below. For details about calling this method, see Calling NetrDatabaseSync2 in section [3.4.5.4.2](#Section_b9acd7feee244bb0a3ff085c4b98284d).

In processing the NetrDatabaseDeltas call, the PDC MAY[<259>](#Appendix_A_259" \o "Product behavior note 259) indicate to the caller that it's unable to fulfill the partial synchronization request due to local conditions. The BDC MUST handle the error by performing full synchronization as described below.

When processing NetrDatabaseSync, NetrDatabaseSync2, or NetrDatabaseDeltas calls, the PDC MUST update the AbstractBdcDatabaseSerialNumbers element corresponding to the database of the BDC making the call to be equal to the value of the [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) for the last database record returned by the call.

#### Message Processing on BDC

Upon receiving an announcement message, the BDC MUST process the message as follows.

* The BDC MUST validate the message to fully conform to the format of the announcement message, and extract all of the message fields.
* The BDC MUST validate that the value of **DomainName** is equal to the value of AbstractDomainName encoded in the [**OEM character set**](#gt_3240e34e-920e-40ac-a672-342ac34a5e22). If the value is different, the BDC MUST ignore the message as invalid.
* The BDC MUST validate that the value of **DomainSid** is equal to the value of AbstractDomainSid. If the value is different, the BDC MUST ignore the message as invalid.
* The BDC MUST determine that a synchronization request is needed if one of the following conditions is true:
  + The value of **DateAndTime** of one of the **DBChangeInfo** fields is not equal to the local value of the corresponding abstract [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) creation time (AbstractSamDatabaseCreationTime, AbstractBuiltinDatabaseCreationTime, or AbstractLsaDatabaseCreationTime). If this condition is true, the BDC MUST set to TRUE the corresponding Boolean value (AbstractFullSamSynchronizationNeeded, AbstractFullBuiltinSynchronizationNeeded, or AbstractFullLsaSynchronizationNeeded) to indicate that a full synchronization is needed for the corresponding database.
  + The value of **LargeSerialNumber** of one of the **DBChangeInfo** fields is not equal to the local value of the corresponding abstract [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) (AbstractSamDatabaseSerialNumber, AbstractBuiltinDatabaseSerialNumber, or AbstractLsaDatabaseSerialNumber). If this condition is true, the BDC MUST set to FALSE the corresponding Boolean value (AbstractFullSamSynchronizationNeeded, AbstractFullBuiltinSynchronizationNeeded, or AbstractFullLsaSynchronizationNeeded) to indicate that a partial ([**delta**](#gt_bac72edb-4ce9-4baa-8977-f33e331b2b5e)) synchronization is needed for the corresponding database.
* If a synchronization request is needed, the BDC MUST set the BDC timer to expire in the amount of time equal to a random value between zero and the value of the Random field.

### Timer Events

#### Timer Events on PDC

When the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) timer expires, the PDC MUST prepare the announcement message (as specified in section [2.2.1.5.1](#Section_b3a7e5f3d6694f54acb8e85580eaf46d)) using the current [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) state, and send the message to BDCs that need synchronization. A BDC needs database synchronization if one of the following conditions is true:

* The announcement is forced as a result of administrative action.

The announcement can be forced if this is a new BDC configured in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca).

* The BDC [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) is less than the PDC database serial number for the corresponding database as indicated by an AbstractBdcDatabaseSerialNumbers element corresponding to the BDC and the database. To prevent sending messages to slow or unreachable BDCs, this condition MAY[<260>](#Appendix_A_260" \o "Product behavior note 260) be augmented to require that the BDC finishes processing the previous announcement (if any), or it is timed out before the PDC sends a new announcement message.
* More than AbstractMaximumPulse seconds passed since the BDC was sent the previous announcement message.

To reduce the load on the PDC from synchronization requests following the PDC announcement, the PDC sends messages only if the current value of AbstractPulseConcurrency is less than a certain value defined as a configuration setting.

The PDC resets its timer to expire in the AbstractPulse seconds.

#### Timer Events on BDC

When the BDC timer expires, the BDC MUST synchronize all its [**databases**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) as follows.

##### Full Synchronization

[**Full database synchronization**](#gt_40bb6bec-5505-4967-b4ad-371f47cd70c9) is performed if the corresponding Boolean value (AbstractFullSamSynchronizationNeeded, AbstractFullBuiltinSynchronizationNeeded, or AbstractFullLsaSynchronizationNeeded) is TRUE. If F is set in the NegotiatedFlags, the BDC MUST call [NetrDatabaseSync2](#Section_31fc80bd4f4d4512a792e488bb78f6a0); otherwise the BDC will call [NetrDatabaseSync](#Section_86683ada19a2414eafaf124f77dc4685) until all changes are obtained for the corresponding [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). After successfully receiving the changes, the BDC MUST update local database to bring it in sync with the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). The BDC MUST update the value of the abstract [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) for the corresponding database (AbstractSamDatabaseSerialNumber, AbstractBuiltinDatabaseSerialNumber, or AbstractLsaDatabaseSerialNumber) and the abstract database creation time (AbstractSamDatabaseCreationTime, AbstractBuiltinDatabaseCreationTime, or AbstractLsaDatabaseCreationTime) to equal to the corresponding value from the PDC as follows:

* The values are set depending on the value of the **DeltaType** field of the last NETLOGON\_DELTA\_ENUM (section [2.2.1.5.11](#Section_20e5863c014240f6a914f352a9d66047)) element in the **Deltas** field of the NETLOGON\_DELTA\_ENUM\_ARRAY (section [2.2.1.5.12](#Section_82d47318c4d8458386a6ce186504bcba)) structure that is one of the following values:
  + If **DeltaType** is AddOrChangeDomain, the abstract database serial number and the abstract database creation time values MUST set to the **DomainModifiedCount** and **DomainCreationTime** fields, respectively, of the NETLOGON\_DELTA\_DOMAIN structure (section [2.2.1.5.10](#Section_803be876d7554187a011eaf5bf2755ab)).
  + If **DeltaType** is AddOrChangeLsaPolicy, the abstract database serial number and the abstract database creation time values MUST be set to the **ModifiedId** and **DatabaseCreationTime** fields, respectively, of the NETLOGON\_DELTA\_POLICY structure (section [2.2.1.5.19](#Section_b9ee3608efd14d57b4da5a13b9ec1fa1)).

##### Partial Synchronization

[**Partial database synchronization**](#gt_42f272ce-e299-4182-b2b2-a3c8d2ffe4db) is performed if the corresponding Boolean value (AbstractFullSamSynchronizationNeeded, AbstractFullBuiltinSynchronizationNeeded, or AbstractFullLsaSynchronizationNeeded) is FALSE. In that case, the BDC MUST call [NetrDatabaseDeltas](#Section_5412f0bc5eb94197b4c4c5a8c06ba018) in a loop until all changes are obtained for the corresponding [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15). After successfully receiving the changes, the BDC MUST update the local database to bring it in sync with the [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). The BDC sets the value of the abstract [**database serial number**](#gt_0b04ee8e-be04-4d04-94c4-90e58390f83d) for the corresponding database (AbstractSamDatabaseSerialNumber, AbstractBuiltinDatabaseSerialNumber, or AbstractLsaDatabaseSerialNumber) to the value of the *DomainModifiedCount* parameter returned by the last NetrDatabaseDeltas call in the replication loop.

If a NetrDatabaseDeltas call returns a status code 0xC0000134, the BDC MUST fully synchronize its entire database as described previously. The BDC performs a full synchronization on receiving any error code other than STATUS\_SUCCESS or STATUS\_ACCESS\_DENIED.

For either synchronization type, the BDC resets its timer to never expire at the end of processing.

### Other Local Events

Administrative actions SHOULD[<261>](#Appendix_A_261" \o "Product behavior note 261) cause [**full database synchronization**](#gt_40bb6bec-5505-4967-b4ad-371f47cd70c9) for all or some BDCs. For example, a configuration change promoting a server to a BDC can result in full database synchronization for that BDC. Similarly, a configuration change to elect a new [**PDC**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d) SHOULD result in full database synchronization for all BDCs. If the accounts [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) becomes corrupt, it SHOULD be recovered via a full synchronization request.

# Protocol Examples

The Netlogon Remote Protocol methods are simple client/server [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) methods in which the client calls the method and the server returns a response. In establishing the connection with the server, the methods have two flows of operation:

* Not requiring a [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) establishment.
* Requiring a session key establishment (often referred to as establishing a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca)).

If a method does not require a session key establishment, the flow of operations will be as specified in section [3.1.4.7](#Section_6b7f7a1c83b7452c9b7b2ece221e236d). The server will return a response whenever a method is called by the client.

When a method requires a session key establishment, the flow of operations to establish a secure channel will be as specified in section [3.1.4.6](#Section_f61c3f4a53ff4f3090066d93a2162ef8). RPC will use the Netlogon SSP to protect the method. The Netlogon SSP protects the data using the negotiated session key. The server will return a response whenever a method is called by the client.

The following section describes an example of pass-through authentication to illustrate the function of this protocol and values that can be used to test session key validation cryptography.

## NetrLogonSamLogon with Secure Channel

When a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is required, a number of additional steps are taken in the process of executing the method. For example, if a client calls the [NetrLogonSamLogon](#Section_a3a192c800704ae3a537dfe0a144426a) method to execute an interactive account logon, the execution of the method involves several steps.

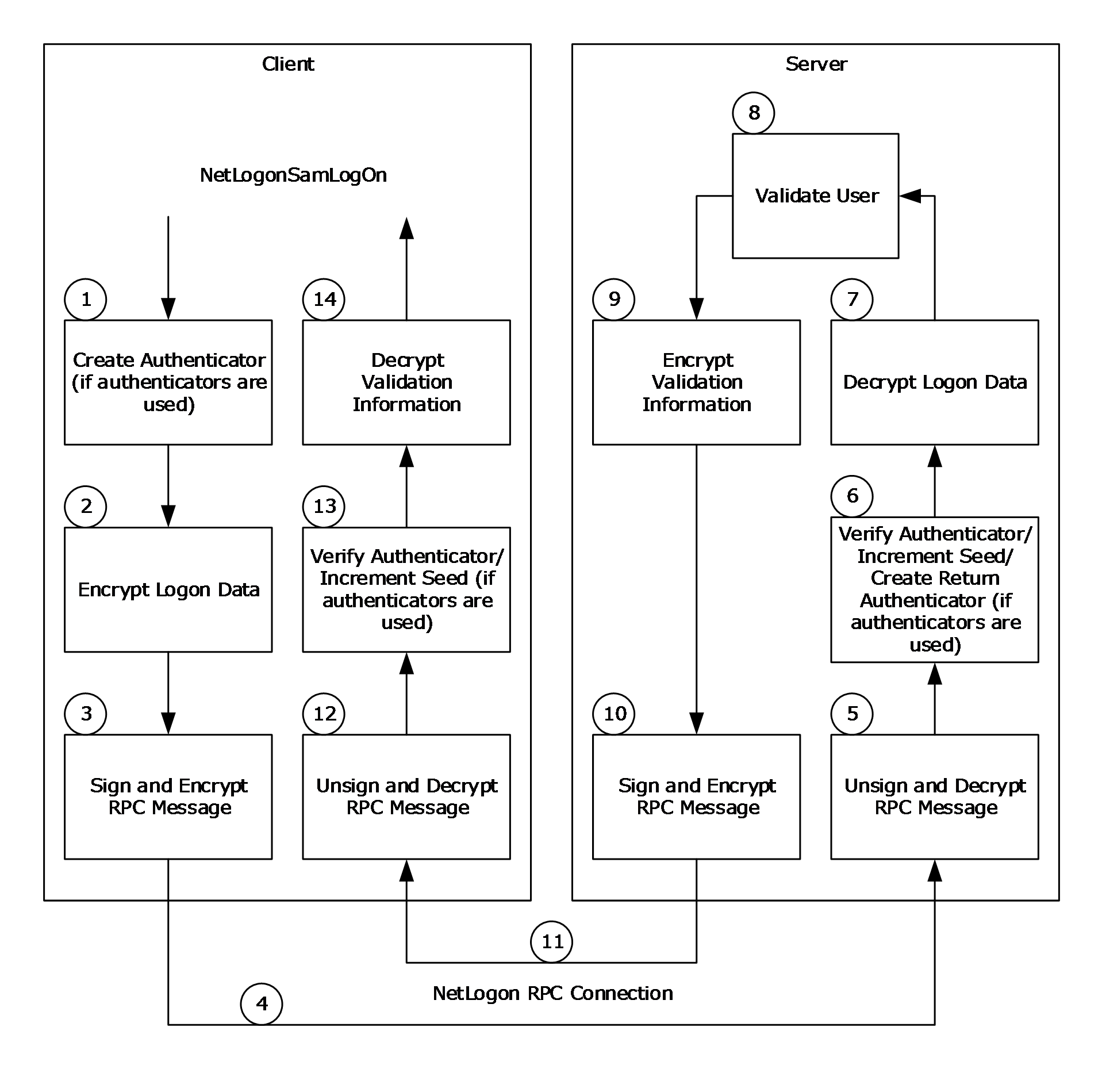


Figure 10: Secure channel execution of NetrLogonSamLogon

NetrLogonSamLogon involves the following steps:

1. If the Netlogon [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) call is using [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3), the following steps are also performed.
   1. The client creates an authenticator. An authenticator is represented by a [NETLOGON\_AUTHENTICATOR](#Section_76c93227942a4687ab9d9d972ffabdab) structure.
   2. The client fills in the timestamp field of the structure with the number of seconds since 00:00:00 on January 1, 1970 (UTC). The client then adds this value to the current authentication seed to produce a new seed value.
   3. The client computes the [**credential**](#gt_b505ab37-868d-426c-bb19-af21e675e0b8) based on the new authentication seed, the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d), and the [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473), per the calculation specified in the previous Netlogon Credentials section.
2. If the *LogonLevel* parameter of the NetrLogonSamLogon method contained one of a set of particular values, the client encrypts the logon data using the session key with the negotiated encryption algorithm. The following table defines the *LogonLevel* parameter value and the data that is encrypted.

| LogonLevel value | Data encrypted |
| --- | --- |
| NetlogonInteractiveInformation (1) | The **LmOwfPassword** and **NtOwfPassword** fields of the [NETLOGON\_INTERACTIVE\_INFO](#Section_af76351fef6946bca451e4c4b99bac4a) structure that was passed in the *LogonInformation* parameter. |
| NetlogonInteractiveTransitiveInformation (5) | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_INTERACTIVE\_INFO structure that was passed in the *LogonInformation* parameter. |
| NetlogonServiceInformation (3) | The **LmOwfPassword** and **NtOwfPassword** fields of the [NETLOGON\_SERVICE\_INFO](#Section_1c9f2af2e16445489428eae68a03537e) structure that was passed in the *LogonInformation* parameter. |
| NetlogonServiceTransitiveInformation (7) | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_SERVICE\_INFO structure that was passed in the *LogonInformation* parameter. |
| NetlogonGenericInformation (4) | The contents of the **LogonData** buffer of the [NETLOGON\_GENERIC\_INFO](#Section_c03d6d959b5e43299645eedcdd167f6e) structure that was passed in the *LogonInformation* parameter. |

This step is not performed for any other *LogonLevel* parameter values.

1. The client signs and encrypts the RPC message. The data is first passed to RPC, where it is formatted according to the RPC standard. RPC then calls back to Netlogon to encrypt the RPC data buffer. The encryption of the RPC data buffer includes the following steps. (The checksum algorithm used is the negotiated checksum algorithm. The encryption algorithm used is the negotiated encryption algorithm.)
   1. Create and initialize a signature. A signature is represented by an [NL\_AUTH\_SIGNATURE](#Section_05b99afd1b6a4207b16e959e6a483867) structure.
   2. Generate random data for the confounder in the signature.
   3. Assign the sequence number in the signature based on the [**nonce**](#gt_001c0e40-0980-417d-853c-f7cb34ba6d3b), and increment the nonce.

**Note**  The nonce is initialized to zero and is used to maintain the sequence number for the calls over the secure channel.

* 1. Calculate the checksum of the first 8 bytes of the signature.
  2. Calculate the checksum of the 8 bytes that make up the confounder in the signature.
  3. Create an [**encryption key**](#gt_fbdcfa70-e954-4dbd-bafa-0f9c4bcf90dd) by using exclusive OR to join the session key with 0x0F0F0F0F.
  4. Encrypt the confounder using the encryption key.
  5. Calculate the checksum of the caller's message.
  6. Encrypt the caller's message using the encryption key.
  7. Finalize the checksum and assign it to the checksum in the signature.
  8. Encrypt the sequence number in the signature using the session key.

1. The client sends the data over the Netlogon RPC connection.
2. The server verifies the signature and decrypts the RPC message. The [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) of the RPC message includes the following steps:
   1. Decrypt the sequence number in the signature using the session key.
   2. Compare the sequence number with the nonce, and increment the nonce.
   3. Calculate the checksum of the first 8 bytes of the signature.
   4. Create an encryption key by XOR'ing the session key with 0x0F0F0F0F.
   5. Decrypt the confounder using the encryption key.
   6. Calculate the checksum of the 8 bytes that make up the confounder in the signature.
   7. Decrypt the caller's message using the encryption key.
   8. Calculate the checksum of the caller's message.
   9. Finalize the checksum and compare it with the checksum in the signature.
3. If the Netlogon RPC call is using authenticators, the server verifies the received authenticator and creates a return authenticator. To verify the received authenticator, the server adds the time stamp value in the authenticator to the current authentication seed to produce a new seed value. The server then computes the client's credential based on the new authentication seed, the session key, and the client challenge, per the calculation specified in the previous Netlogon Credentials section. Finally, the server checks whether the resulting credential is equal to the credential in the received authenticator. If successful, the server adds 1 to the authentication seed. Then the server creates a return authenticator. The server computes the credential for the return authenticator based on the new authentication seed, the session key, and the [**server challenge (SC)**](#gt_7deccd83-29bf-4f63-ba8d-d3ae04d196e9), per the calculation specified in the previous Netlogon Credentials section.
4. If the *LogonLevel* parameter of the NetrLogonSamLogon method contained one of a set of particular values, the server decrypts the logon data, using the session key with the negotiated decryption algorithm. The following table defines the *LogonLevel* parameter values and the data that is decrypted.

| LogonLevel value | Data decrypted |
| --- | --- |
| 1 | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_INTERACTIVE\_INFO structure that was passed in the *LogonInformation* parameter. |
| 5 | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_INTERACTIVE\_INFO structure that was passed in the *LogonInformation* parameter. |
| 3 | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_SERVICE\_INFO structure that was passed in the *LogonInformation* parameter. |
| 7 | The **LmOwfPassword** and **NtOwfPassword** fields of the NETLOGON\_SERVICE\_INFO structure that was passed in the *LogonInformation* parameter. |
| 4 | The contents of the **LogonData** buffer of the NETLOGON\_GENERIC\_INFO structure that was passed in the *LogonInformation* parameter. |

This step is not performed for any other *LogonLevel* parameter values.

1. The server executes its implementation of the NetrLogonSamLogon method to validate the user. The resulting validation information is returned in a [NETLOGON\_VALIDATION](#Section_5eb0b7cb3a55477b92fcc236bd5873fa) union.
2. If the *LogonLevel* parameter of the NetrLogonSamLogon method contained one of the following values, the server encrypts the validation information:
   * NetlogonNetworkInformation
   * NetlogonNetworkTransitiveInformation
   * NetlogonGenericInformation

The validation data is encrypted using the session key with the negotiated encryption algorithm. The data that is encrypted depends on the value that was passed in the *ValidationLevel* parameter of the NetrLogonSamLogon method. The following table defines the *ValidationLevel* parameter values and the data that is encrypted.

| ValidationLevel value | Data encrypted |
| --- | --- |
| 2 | The **UserSessionKey** and **ExpansionRoom** fields of the [NETLOGON\_VALIDATION\_SAM\_INFO](#Section_142a277fe16145ac8b95b94bb169b5da) structure, as specified in section 2.2.1.4.11, that was passed in the *ValidationInformation* parameter. |
| 3 | The **UserSessionKey** and **ExpansionRoom** fields of the [NETLOGON\_VALIDATION\_SAM\_INFO2](#Section_2a12e28979044ecb9d836732200230c0) structure, as specified in section 2.2.1.4.12, that was passed in the *ValidationInformation* parameter. |
| 5 | The contents of the **ValidationData** buffer of the [NETLOGON\_VALIDATION\_GENERIC\_INFO2](#Section_e89f8f5b098541a0b1101ae0ea2bd183) structure, as specified in section 2.2.1.4.8, that was passed in the *ValidationInformation* parameter. |

This step is not performed for any other *LogonLevel* parameter values.

1. The server signs and encrypts the RPC response message. The server performs the same steps as the client performed in step 3.
2. The server sends the response back to client over the Netlogon RPC connection.
3. The client unsigns and decrypts the RPC message. The client performs the same steps as the server performed in step 5.
4. If the Netlogon RPC call is using authenticators, the client verifies the return authenticator. To verify the return authenticator, the client adds 1 to the authentication seed to produce a new seed value. The client then computes the server's credential based on the new authentication seed, the session key, and the server challenge, per the calculation specified in the previous Netlogon Credentials section. Finally, the client checks whether the resulting credential is equal to the credential in the return authenticator.
5. If the *LogonLevel* parameter of the NetrLogonSamLogon method contained one of the following values, the client decrypts the validation information:
   * NetlogonNetworkInformation
   * NetlogonNetworkTransitiveInformation
   * NetlogonGenericInformation

The validation data is decrypted using the session key with the negotiated decryption algorithm. The data that is decrypted depends on the value that was passed in the *ValidationLevel* parameter of the NetrLogonSamLogon method. The following table defines the *ValidationLevel* parameter value and the data that is decrypted.

| ValidationLevel value | Data decrypted |
| --- | --- |
| 2 | The **UserSessionKey** and **ExpansionRoom** fields of the NETLOGON\_VALIDATION\_SAM\_INFO structure, as specified in section 2.2.1.4.11, that was passed in the *ValidationInformation* parameter. |
| 3 | The **UserSessionKey** and **ExpansionRoom** fields of the NETLOGON\_VALIDATION\_SAM\_INFO2 structure, as specified in section 2.2.1.4.12, that was passed in the *ValidationInformation* parameter. |
| 5 | The contents of the **ValidationData** buffer of the NETLOGON\_VALIDATION\_GENERIC\_INFO2 structure, as specified in section 2.2.1.4.8, that was passed in the *ValidationInformation* parameter. |

This step is not performed for all other *LogonLevel* parameter values.

The execution of all other Netlogon methods requiring a secure channel is similar to the previous example.

## Cryptographic Values for Session Key Validation

The following values were obtained from a Kernel debugger dump. They can be used when validating [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) negotiation code.

Clear-text **SharedSecret** (machine password):

1. 0000000: 2e 00 2f 00 2c 00 6e 00 4c 00 3e 00 4f 00 4c 00 ../.,.n.L.>.O.L.
2. 0000010: 5a 00 36 00 73 00 74 00 5e 00 58 00 4b 00 65 00 Z.6.s.t.^.X.K.e.
3. 0000020: 4d 00 25 00 2e 00 49 00 2d 00 74 00 45 00 60 00 M.%...I.-.t.E.`.
4. 0000030: 57 00 56 00 6a 00 43 00 5b 00 30 00 36 00 3f 00 W.V.j.C.[.0.6.?.
5. 0000040: 5d 00 3a 00 51 00 76 00 5f 00 54 00 6e 00 55 00 ].:.Q.v.\_.T.n.U.
6. 0000050: 6f 00 3a 00 3a 00 42 00 77 00 2c 00 67 00 60 00 o.:.:.B.w.,.g.`.
7. 0000060: 76 00 23 00 4a 00 4d 00 36 00 4d 00 71 00 53 00 v.#.J.M.6.M.q.S.
8. 0000070: 50 00 75 00 55 00 28 00 6e 00 71 00 34 00 3e 00 P.u.U.(.n.q.4.>.
9. 0000080: 79 00 6a 00 5b 00 64 00 5c 00 2b 00 56 00 70 00 y.j.[.d.\.+.V.p.
10. 0000090: 52 00 5f 00 79 00 78 00 75 00 63 00 21 00 67 00 R.\_.y.x.u.c.!.g.
11. 00000a0: 30 00 54 00 36 00 35 00 76 00 7a 00 57 00 41 00 0.T.6.5.v.z.W.A.
12. 00000b0: 42 00 5f 00 42 00 22 00 69 00 3c 00 3c 00 53 00 B.\_.B.".i.<.<.S.
13. 00000c0: 2b 00 34 00 27 00 5e 00 3a 00 21 00 2c 00 3b 00 +.4.'.^.:.!.,.;.
14. 00000d0: 25 00 47 00 73 00 2d 00 28 00 22 00 3a 00 20 00 %.G.s.-.(.".:. .
15. 00000e0: 6d 00 3e 00 21 00 43 00 4c 00 66 00 6e 00 4e 00 m.>.!.C.L.f.n.N.

OWF of **SharedSecret**:

1. 0000000: 31 a5 90 17 0a 35 1f d5-11 48 b2 a1 0a f2 c3 05 1....5...H......

Client Challenge:

1. 0000000: 3a 03 90 a4 6d 0c 3d 4f :...m.=O

Server Challenge:

1. 0000000: 0c 4c 13 d1 60 41 c8 60 .L..`A.`

Session Key:

1. 0000000: ee fe 8f 40 00 7a 2e eb-68 43 d0 d3 0a 5b e2 e3 ...@.z..hC...[..

### ASCII MD4 Testing

The following cryptographic values are provided to test using the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to produce MD4 outputs with ASCII inputs.

Input:

1. 0000000: 74 65 73 74 test

Output:

1. 0000000: db 34 6d 69 1d 7a cc 4d c2 62 5d b1 9f 9e 3f 52 .4mi.z.M.b]...?R

### UNICODE MD4 Testing

The following cryptographic values are provided to test using the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d) to produce MD4 outputs with UNICODE inputs.

Input:

1. 0000000: 74 00 65 00 73 00 74 00 t.e.s.t.

Output:

1. 0000000: 0c b6 94 88 05 f7 97 bf 2a 82 80 79 73 b8 95 37 ........\*..ys..7

# Security Considerations

## Security Considerations for Implementers

Security considerations for both unauthenticated [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) and Secure RPC, as used in this protocol, are as specified in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) sections 5.1 and 5.2.

When the Netlogon Remote Protocol [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) was originally implemented, only certain security-sensitive RPC call arguments, such as passwords, were encrypted. This mechanism involved passing extra parameters, known as [**authenticators**](#gt_e72a2c02-84a2-4ce3-b66f-86f725642dc3), as RPC call arguments; these are used for authenticating the RPC calls. Later, support was added to sign and encrypt the entire RPC message with the help of a new Netlogon Remote Protocol security package. However, the encryption and validation of individual security-sensitive parameters, and the use of authenticators that are passed as RPC-call arguments for authenticating the calls, were preserved in the existing RPC calls, even though these were redundant at that point.

On receiving the [DsrDeregisterDnsHostRecords](#Section_db6c9aad573640c5af86538dd439134c) call, the server should control access to this method. Because DsrDeregisterDnsHostRecords deletes [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) records for any specific [**DC**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd), the client should have administrative [**privileges**](#gt_d8092e10-b227-4b44-b015-511bb8178940) (such as those Administrator, Local System, Account Operator, or System Operator accounts have) for the call to succeed.

One of the new RPC calls that was added later, [NetrLogonSamLogonEx](#Section_1725735133844de5bfe0453926ef67cd), does not use authenticators. Instead, it encrypts the entire RPC message when encryption is requested. NetrLogonSamLogonEx is currently the only RPC call that is made over a secure channel that does not use authenticators. The presence of authenticators is determined by the Netlogon Remote Protocol call that was made.

To prevent remote denial of service (DoS) attacks, the server can delete the stored *ServerChallenge*, client name and [**client challenge**](#gt_54ceb15a-5c0f-4099-8d9f-71f7b91b0473) used for the [NetrServerReqChallenge](#Section_5ad9db9f74414ce58c7b7b771e243d32) method after a couple of minutes.

To prevent information disclosure, the server should control access to the [DsrGetForestTrustInformation](#Section_8bff4d0be06c4c3a8bd9b0e2a7f2b06b) method to authenticated users.

To prevent information disclosure, the client should be a registered user of the corporate [**forest**](#gt_fd104241-4fb3-457c-b2c4-e0c18bb20b62) for the local computer account [**RID**](#gt_df3d0b61-56cd-4dac-9402-982f1fedc41c) and limited to only those clients (such as local system or members of the local administrators [**group**](#gt_51c51c14-7f9d-4c0b-a69c-d3e059bfffac)) that need the RID for a [**trust**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) account for the [NetrLogonGetTrustRid](#Section_1d6fad9e763d495f9bed18c79304c3d7) call to succeed.

On receiving the [NetrLogonComputeServerDigest](#Section_5f95c374795142d9816cc7f4cff2ed52) call, the server should control access to this method. Because NetrLogonComputeServerDigest is an administrative method, the client should have administrative privileges (such as those the local administrators group, local system, or local service have) for the call to succeed.

On receiving the [NetrLogonComputeClientDigest](#Section_79ca6e90ccd2429eb5ac8050b620eef6) call, the server should control access to this method. Because NetrLogonComputeClientDigest is an administrative method, the client should have administrative privileges (such as those the local administrators group, local system, or local service have) for the call to succeed.

On receiving the [NetrLogonSetServiceBits](#Section_481bb1f8319a40fb89cdad1f6a146d9d) call, the server should control access to this method. Because NetrLogonSetServiceBits is an administrative method, the client should have administrative privileges (such as those the local administrators group, local system, or local service have) for the call to succeed.

On receiving the [NetrLogonGetTimeServiceParentDomain](#Section_be27686c237347439b655c97b2618bdd) call, the server should control access to this method to determine whether the caller can access the parent [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca). To prevent information disclosure, the client should have administrative privileges (such as those the local administrators group, local system, or local service have) for the call to succeed.

The server should control access to the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method to determine whether the caller can manage the Netlogon service (the caller requires administrative privileges such as those the local administrators group, local system, or local service have).

The following sections specify security considerations for implementers of the Netlogon Remote Protocol.

## Index of Security Parameters

| Security parameter | Section |
| --- | --- |
| SealSecureChannel | [3.1.1](#Section_708b71329e72447c992bd0bef4078f81) |
| Session Key Parameters | 3.1.1 |
| Netlogon Negotiable Options | [3.1.4.2](#Section_5805bc9fe4c94c8ab1913c3a7de7eeed) |
| Session-Key Computation | [3.1.4.3](#Section_5e9798475b2a4148b6e9047c65a8ae63) |
| Netlogon Credential Computation | [3.1.4.4](#Section_594909fd725f45ac979962e4aefe0585) |
| Netlogon Authenticator Computation and Verification | [3.1.4.5](#Section_da7acaa3030b481e979bf58f89389806) |
| Session-Key Negotiation | [3.1.4.1](#Section_7b9e31d1670e4fc5ad549ffff50755f9) |
| Integrity | [3.3.1](#Section_a7bd20030d614686aa6e89336cec83a1) |
| Sequence Detect | 3.3.1 |
| Confidentiality | 3.3.1 |
| Netlogon Security Context Establishment | [3.3.4.1](#Section_b28a01cb295d4833bdb6b113baf109b4) |
| NL\_AUTH\_MESSAGE | 3.3.4.1 |
| Signing and Encrypting | [3.3.4.2](#Section_2af2dc5f794143aba6d063161a591a6e) |
| NL\_AUTH\_SIGNATURE | 3.3.4.2 |
| domain-name | [3.4.1](#Section_fd1e918135a045d3b39cb7453dfc0af5) |

# Appendix A: Full IDL

For ease of implementation, the full IDL is provided, where "ms-dtyp.idl" refers to the IDL found in [[MS-DTYP]](%5bMS-DTYP%5d.pdf#Section_cca2742956894a16b2b49325d93e4ba2) Appendix A.

The syntax uses the [**IDL**](#gt_73177eec-4092-420f-92c5-60b2478df824) syntax extensions defined in [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15) sections 2.2.4 and 3.1.1.5.1. For example, as noted in [MS-RPCE] section 2.2.4.9, a pointer\_default declaration is not required and pointer\_default(unique) is assumed.

1. import "ms-dtyp.idl";
2. [
3. uuid(12345678-1234-ABCD-EF00-01234567CFFB),
4. version(1.0),
5. ms\_union,
6. pointer\_default(unique)
7. ]
8. interface logon
9. {
10. typedef struct \_STRING{
11. USHORT Length;
12. USHORT MaximumLength;
13. [size\_is(MaximumLength), length\_is(Length) ] CHAR \* Buffer;
14. } STRING, \*PSTRING;
15. typedef struct \_OLD\_LARGE\_INTEGER{
16. ULONG LowPart;
17. LONG HighPart;
18. } OLD\_LARGE\_INTEGER, \*POLD\_LARGE\_INTEGER;
19. typedef struct \_CYPHER\_BLOCK{
20. CHAR data[8];
21. } CYPHER\_BLOCK, \*PCYPHER\_BLOCK;
22. typedef struct \_NT\_OWF\_PASSWORD{
23. CYPHER\_BLOCK data[2];
24. }NT\_OWF\_PASSWORD, \*PNT\_OWF\_PASSWORD,
25. ENCRYPTED\_NT\_OWF\_PASSWORD, \*PENCRYPTED\_NT\_OWF\_PASSWORD;
26. typedef struct \_LM\_OWF\_PASSWORD{
27. CYPHER\_BLOCK data[2];
28. } LM\_OWF\_PASSWORD, \*PLM\_OWF\_PASSWORD,
29. ENCRYPTED\_LM\_OWF\_PASSWORD, \*PENCRYPTED\_LM\_OWF\_PASSWORD;
30. typedef [handle] wchar\_t \* LOGONSRV\_HANDLE;
31. typedef struct \_NLPR\_SID\_INFORMATION{
32. PRPC\_SID SidPointer;
33. } NLPR\_SID\_INFORMATION, \*PNLPR\_SID\_INFORMATION;
34. typedef struct \_NLPR\_SID\_ARRAY{
35. ULONG Count;
36. [size\_is(Count)] PNLPR\_SID\_INFORMATION Sids;
37. } NLPR\_SID\_ARRAY, \*PNLPR\_SID\_ARRAY;
38. typedef struct \_NLPR\_CR\_CIPHER\_VALUE{
39. ULONG Length;
40. ULONG MaximumLength;
41. [size\_is(MaximumLength), length\_is(Length)]
42. UCHAR \* Buffer;
43. } NLPR\_CR\_CIPHER\_VALUE, \*PNLPR\_CR\_CIPHER\_VALUE;
44. typedef struct \_NLPR\_LOGON\_HOURS{
45. USHORT UnitsPerWeek;
46. [size\_is(1260), length\_is((UnitsPerWeek+7)/8)]
47. UCHAR \* LogonHours;
48. } NLPR\_LOGON\_HOURS, \*PNLPR\_LOGON\_HOURS;
49. typedef struct \_NLPR\_USER\_PRIVATE\_INFO{
50. UCHAR SensitiveData;
51. ULONG DataLength;
52. [size\_is(DataLength)] UCHAR \* Data;
53. } NLPR\_USER\_PRIVATE\_INFO, \*PNLPR\_USER\_PRIVATE\_INFO;
54. typedef struct \_NLPR\_MODIFIED\_COUNT{
55. OLD\_LARGE\_INTEGER ModifiedCount;
56. } NLPR\_MODIFIED\_COUNT, \*PNLPR\_MODIFIED\_COUNT;
57. typedef struct \_NLPR\_QUOTA\_LIMITS{
58. ULONG PagedPoolLimit;
59. ULONG NonPagedPoolLimit;
60. ULONG MinimumWorkingSetSize;
61. ULONG MaximumWorkingSetSize;
62. ULONG PagefileLimit;
63. OLD\_LARGE\_INTEGER Reserved;
64. } NLPR\_QUOTA\_LIMITS,
65. \*PNLPR\_QUOTA\_LIMITS;
66. typedef struct \_NETLOGON\_DELTA\_USER{
67. RPC\_UNICODE\_STRING UserName;
68. RPC\_UNICODE\_STRING FullName;
69. ULONG UserId;
70. ULONG PrimaryGroupId;
71. RPC\_UNICODE\_STRING HomeDirectory;
72. RPC\_UNICODE\_STRING HomeDirectoryDrive;
73. RPC\_UNICODE\_STRING ScriptPath;
74. RPC\_UNICODE\_STRING AdminComment;
75. RPC\_UNICODE\_STRING WorkStations;
76. OLD\_LARGE\_INTEGER LastLogon;
77. OLD\_LARGE\_INTEGER LastLogoff;
78. NLPR\_LOGON\_HOURS LogonHours;
79. USHORT BadPasswordCount;
80. USHORT LogonCount;
81. OLD\_LARGE\_INTEGER PasswordLastSet;
82. OLD\_LARGE\_INTEGER AccountExpires;
83. ULONG UserAccountControl;
84. ENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNtOwfPassword;
85. ENCRYPTED\_LM\_OWF\_PASSWORD EncryptedLmOwfPassword;
86. UCHAR NtPasswordPresent;
87. UCHAR LmPasswordPresent;
88. UCHAR PasswordExpired;
89. RPC\_UNICODE\_STRING UserComment;
90. RPC\_UNICODE\_STRING Parameters;
91. USHORT CountryCode;
92. USHORT CodePage;
93. NLPR\_USER\_PRIVATE\_INFO PrivateData;
94. SECURITY\_INFORMATION SecurityInformation;
95. ULONG SecuritySize;
96. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
97. RPC\_UNICODE\_STRING ProfilePath;
98. RPC\_UNICODE\_STRING DummyString2;
99. RPC\_UNICODE\_STRING DummyString3;
100. RPC\_UNICODE\_STRING DummyString4;
101. ULONG DummyLong1;
102. ULONG DummyLong2;
103. ULONG DummyLong3;
104. ULONG DummyLong4;
105. } NETLOGON\_DELTA\_USER,
106. \*PNETLOGON\_DELTA\_USER;
107. typedef struct \_NETLOGON\_DELTA\_GROUP{
108. RPC\_UNICODE\_STRING Name;
109. ULONG RelativeId;
110. ULONG Attributes;
111. RPC\_UNICODE\_STRING AdminComment;
112. SECURITY\_INFORMATION SecurityInformation;
113. ULONG SecuritySize;
114. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
115. RPC\_UNICODE\_STRING DummyString1;
116. RPC\_UNICODE\_STRING DummyString2;
117. RPC\_UNICODE\_STRING DummyString3;
118. RPC\_UNICODE\_STRING DummyString4;
119. ULONG DummyLong1;
120. ULONG DummyLong2;
121. ULONG DummyLong3;
122. ULONG DummyLong4;
123. } NETLOGON\_DELTA\_GROUP,
124. \*PNETLOGON\_DELTA\_GROUP;
125. typedef struct \_NETLOGON\_DELTA\_GROUP\_MEMBER {
126. [size\_is(MemberCount)] ULONG \* Members;
127. [size\_is(MemberCount)] ULONG \* Attributes;
128. ULONG MemberCount;
129. ULONG DummyLong1;
130. ULONG DummyLong2;
131. ULONG DummyLong3;
132. ULONG DummyLong4;
133. } NETLOGON\_DELTA\_GROUP\_MEMBER,
134. \*PNETLOGON\_DELTA\_GROUP\_MEMBER;
135. typedef struct \_NETLOGON\_DELTA\_ALIAS{
136. RPC\_UNICODE\_STRING Name;
137. ULONG RelativeId;
138. SECURITY\_INFORMATION SecurityInformation;
139. ULONG SecuritySize;
140. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
141. RPC\_UNICODE\_STRING Comment;
142. RPC\_UNICODE\_STRING DummyString2;
143. RPC\_UNICODE\_STRING DummyString3;
144. RPC\_UNICODE\_STRING DummyString4;
145. ULONG DummyLong1;
146. ULONG DummyLong2;
147. ULONG DummyLong3;
148. ULONG DummyLong4;
149. } NETLOGON\_DELTA\_ALIAS,
150. \*PNETLOGON\_DELTA\_ALIAS;
151. typedef struct \_NETLOGON\_DELTA\_ALIAS\_MEMBER{
152. NLPR\_SID\_ARRAY Members;
153. ULONG DummyLong1;
154. ULONG DummyLong2;
155. ULONG DummyLong3;
156. ULONG DummyLong4;
157. } NETLOGON\_DELTA\_ALIAS\_MEMBER,
158. \*PNETLOGON\_DELTA\_ALIAS\_MEMBER;
159. typedef struct \_NETLOGON\_DELTA\_DOMAIN{
160. RPC\_UNICODE\_STRING DomainName;
161. RPC\_UNICODE\_STRING OemInformation;
162. OLD\_LARGE\_INTEGER ForceLogoff;
163. USHORT MinPasswordLength;
164. USHORT PasswordHistoryLength;
165. OLD\_LARGE\_INTEGER MaxPasswordAge;
166. OLD\_LARGE\_INTEGER MinPasswordAge;
167. OLD\_LARGE\_INTEGER DomainModifiedCount;
168. OLD\_LARGE\_INTEGER DomainCreationTime;
169. SECURITY\_INFORMATION SecurityInformation;
170. ULONG SecuritySize;
171. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
172. RPC\_UNICODE\_STRING DomainLockoutInformation;
173. RPC\_UNICODE\_STRING DummyString2;
174. RPC\_UNICODE\_STRING DummyString3;
175. RPC\_UNICODE\_STRING DummyString4;
176. ULONG PasswordProperties;
177. ULONG DummyLong2;
178. ULONG DummyLong3;
179. ULONG DummyLong4;
180. } NETLOGON\_DELTA\_DOMAIN,
181. \*PNETLOGON\_DELTA\_DOMAIN;
182. typedef struct \_NETLOGON\_DELTA\_RENAME\_GROUP{
183. RPC\_UNICODE\_STRING OldName;
184. RPC\_UNICODE\_STRING NewName;
185. RPC\_UNICODE\_STRING DummyString1;
186. RPC\_UNICODE\_STRING DummyString2;
187. RPC\_UNICODE\_STRING DummyString3;
188. RPC\_UNICODE\_STRING DummyString4;
189. ULONG DummyLong1;
190. ULONG DummyLong2;
191. ULONG DummyLong3;
192. ULONG DummyLong4;
193. } NETLOGON\_RENAME\_GROUP,
194. \*PNETLOGON\_DELTA\_RENAME\_GROUP;
195. typedef struct \_NETLOGON\_DELTA\_RENAME\_USER{
196. RPC\_UNICODE\_STRING OldName;
197. RPC\_UNICODE\_STRING NewName;
198. RPC\_UNICODE\_STRING DummyString1;
199. RPC\_UNICODE\_STRING DummyString2;
200. RPC\_UNICODE\_STRING DummyString3;
201. RPC\_UNICODE\_STRING DummyString4;
202. ULONG DummyLong1;
203. ULONG DummyLong2;
204. ULONG DummyLong3;
205. ULONG DummyLong4;
206. } NETLOGON\_RENAME\_USER,
207. \*PNETLOGON\_DELTA\_RENAME\_USER;
208. typedef struct \_NETLOGON\_DELTA\_RENAME\_ALIAS{
209. RPC\_UNICODE\_STRING OldName;
210. RPC\_UNICODE\_STRING NewName;
211. RPC\_UNICODE\_STRING DummyString1;
212. RPC\_UNICODE\_STRING DummyString2;
213. RPC\_UNICODE\_STRING DummyString3;
214. RPC\_UNICODE\_STRING DummyString4;
215. ULONG DummyLong1;
216. ULONG DummyLong2;
217. ULONG DummyLong3;
218. ULONG DummyLong4;
219. } NETLOGON\_RENAME\_ALIAS,
220. \*PNETLOGON\_DELTA\_RENAME\_ALIAS;
221. typedef struct \_NETLOGON\_DELTA\_POLICY{
222. ULONG MaximumLogSize;
223. OLD\_LARGE\_INTEGER AuditRetentionPeriod;
224. UCHAR AuditingMode;
225. ULONG MaximumAuditEventCount;
226. [size\_is(MaximumAuditEventCount + 1)]
227. ULONG \* EventAuditingOptions;
228. RPC\_UNICODE\_STRING PrimaryDomainName;
229. PRPC\_SID PrimaryDomainSid;
230. NLPR\_QUOTA\_LIMITS QuotaLimits;
231. OLD\_LARGE\_INTEGER ModifiedId;
232. OLD\_LARGE\_INTEGER DatabaseCreationTime;
233. SECURITY\_INFORMATION SecurityInformation;
234. ULONG SecuritySize;
235. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
236. RPC\_UNICODE\_STRING DummyString1;
237. RPC\_UNICODE\_STRING DummyString2;
238. RPC\_UNICODE\_STRING DummyString3;
239. RPC\_UNICODE\_STRING DummyString4;
240. ULONG DummyLong1;
241. ULONG DummyLong2;
242. ULONG DummyLong3;
243. ULONG DummyLong4;
244. } NETLOGON\_DELTA\_POLICY,
245. \*PNETLOGON\_DELTA\_POLICY;
246. typedef struct \_NETLOGON\_DELTA\_TRUSTED\_DOMAINS{
247. RPC\_UNICODE\_STRING DomainName;
248. ULONG NumControllerEntries;
249. [size\_is(NumControllerEntries)]
250. PRPC\_UNICODE\_STRING ControllerNames;
251. SECURITY\_INFORMATION SecurityInformation;
252. ULONG SecuritySize;
253. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
254. RPC\_UNICODE\_STRING DummyString1;
255. RPC\_UNICODE\_STRING DummyString2;
256. RPC\_UNICODE\_STRING DummyString3;
257. RPC\_UNICODE\_STRING DummyString4;
258. ULONG TrustedPosixOffset;
259. ULONG DummyLong2;
260. ULONG DummyLong3;
261. ULONG DummyLong4;
262. } NETLOGON\_DELTA\_TRUSTED\_DOMAINS,
263. \*PNETLOGON\_DELTA\_TRUSTED\_DOMAINS;
264. typedef struct \_NETLOGON\_DELTA\_ACCOUNTS{
265. ULONG PrivilegeEntries;
266. ULONG PrivilegeControl;
267. [size\_is(PrivilegeEntries)]
268. ULONG \* PrivilegeAttributes;
269. [size\_is(PrivilegeEntries)] PRPC\_UNICODE\_STRING PrivilegeNames;
270. NLPR\_QUOTA\_LIMITS QuotaLimits;
271. ULONG SystemAccessFlags;
272. SECURITY\_INFORMATION SecurityInformation;
273. ULONG SecuritySize;
274. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
275. RPC\_UNICODE\_STRING DummyString1;
276. RPC\_UNICODE\_STRING DummyString2;
277. RPC\_UNICODE\_STRING DummyString3;
278. RPC\_UNICODE\_STRING DummyString4;
279. ULONG DummyLong1;
280. ULONG DummyLong2;
281. ULONG DummyLong3;
282. ULONG DummyLong4;
283. } NETLOGON\_DELTA\_ACCOUNTS,
284. \*PNETLOGON\_DELTA\_ACCOUNTS;
285. typedef struct \_NETLOGON\_DELTA\_SECRET{
286. NLPR\_CR\_CIPHER\_VALUE CurrentValue;
287. OLD\_LARGE\_INTEGER CurrentValueSetTime;
288. NLPR\_CR\_CIPHER\_VALUE OldValue;
289. OLD\_LARGE\_INTEGER OldValueSetTime;
290. SECURITY\_INFORMATION SecurityInformation;
291. ULONG SecuritySize;
292. [size\_is(SecuritySize)] UCHAR \* SecurityDescriptor;
293. RPC\_UNICODE\_STRING DummyString1;
294. RPC\_UNICODE\_STRING DummyString2;
295. RPC\_UNICODE\_STRING DummyString3;
296. RPC\_UNICODE\_STRING DummyString4;
297. ULONG DummyLong1;
298. ULONG DummyLong2;
299. ULONG DummyLong3;
300. ULONG DummyLong4;
301. } NETLOGON\_DELTA\_SECRET,
302. \*PNETLOGON\_DELTA\_SECRET;
303. typedef struct \_NETLOGON\_DELTA\_DELETE\_GROUP{
304. [string] wchar\_t \* AccountName;
305. RPC\_UNICODE\_STRING DummyString1;
306. RPC\_UNICODE\_STRING DummyString2;
307. RPC\_UNICODE\_STRING DummyString3;
308. RPC\_UNICODE\_STRING DummyString4;
309. ULONG DummyLong1;
310. ULONG DummyLong2;
311. ULONG DummyLong3;
312. ULONG DummyLong4;
313. } NETLOGON\_DELTA\_DELETE\_GROUP,
314. \*PNETLOGON\_DELTA\_DELETE\_GROUP;
315. typedef struct \_NETLOGON\_DELTA\_DELETE\_USER{
316. [string] wchar\_t \* AccountName;
317. RPC\_UNICODE\_STRING DummyString1;
318. RPC\_UNICODE\_STRING DummyString2;
319. RPC\_UNICODE\_STRING DummyString3;
320. RPC\_UNICODE\_STRING DummyString4;
321. ULONG DummyLong1;
322. ULONG DummyLong2;
323. ULONG DummyLong3;
324. ULONG DummyLong4;
325. } NETLOGON\_DELTA\_DELETE\_USER,
326. \*PNETLOGON\_DELTA\_DELETE\_USER;
327. typedef enum \_NETLOGON\_DELTA\_TYPE{
328. AddOrChangeDomain = 1,
329. AddOrChangeGroup = 2,
330. DeleteGroup = 3,
331. RenameGroup = 4,
332. AddOrChangeUser = 5,
333. DeleteUser = 6,
334. RenameUser = 7,
335. ChangeGroupMembership = 8,
336. AddOrChangeAlias = 9,
337. DeleteAlias = 10,
338. RenameAlias = 11,
339. ChangeAliasMembership = 12,
340. AddOrChangeLsaPolicy = 13,
341. AddOrChangeLsaTDomain = 14,
342. DeleteLsaTDomain = 15,
343. AddOrChangeLsaAccount = 16,
344. DeleteLsaAccount = 17,
345. AddOrChangeLsaSecret = 18,
346. DeleteLsaSecret = 19,
347. DeleteGroupByName = 20,
348. DeleteUserByName = 21,
349. SerialNumberSkip = 22
350. } NETLOGON\_DELTA\_TYPE;
351. typedef [switch\_type(NETLOGON\_DELTA\_TYPE)] union
352. \_NETLOGON\_DELTA\_UNION{
353. [case(AddOrChangeDomain)]
354. PNETLOGON\_DELTA\_DOMAIN DeltaDomain;
355. [case(AddOrChangeGroup)]
356. PNETLOGON\_DELTA\_GROUP DeltaGroup;
357. [case(RenameGroup)]
358. PNETLOGON\_DELTA\_RENAME\_GROUP DeltaRenameGroup;
359. [case(AddOrChangeUser)]
360. PNETLOGON\_DELTA\_USER DeltaUser;
361. [case(RenameUser)]
362. PNETLOGON\_DELTA\_RENAME\_USER DeltaRenameUser;
363. [case(ChangeGroupMembership)]
364. PNETLOGON\_DELTA\_GROUP\_MEMBER DeltaGroupMember;
365. [case(AddOrChangeAlias)]
366. PNETLOGON\_DELTA\_ALIAS DeltaAlias;
367. [case(RenameAlias)]
368. PNETLOGON\_DELTA\_RENAME\_ALIAS DeltaRenameAlias;
369. [case(ChangeAliasMembership)]
370. PNETLOGON\_DELTA\_ALIAS\_MEMBER DeltaAliasMember;
371. [case(AddOrChangeLsaPolicy)]
372. PNETLOGON\_DELTA\_POLICY DeltaPolicy;
373. [case(AddOrChangeLsaTDomain)]
374. PNETLOGON\_DELTA\_TRUSTED\_DOMAINS DeltaTDomains;
375. [case(AddOrChangeLsaAccount)]
376. PNETLOGON\_DELTA\_ACCOUNTS DeltaAccounts;
377. [case(AddOrChangeLsaSecret)]
378. PNETLOGON\_DELTA\_SECRET DeltaSecret;
379. [case(DeleteGroupByName)]
380. PNETLOGON\_DELTA\_DELETE\_GROUP DeltaDeleteGroup;
381. [case(DeleteUserByName)]
382. PNETLOGON\_DELTA\_DELETE\_USER DeltaDeleteUser;
383. [case(SerialNumberSkip)]
384. PNLPR\_MODIFIED\_COUNT DeltaSerialNumberSkip;
385. [default] ;
386. } NETLOGON\_DELTA\_UNION,
387. \*PNETLOGON\_DELTA\_UNION;
388. typedef [switch\_type(NETLOGON\_DELTA\_TYPE)] union
389. \_NETLOGON\_DELTA\_ID\_UNION{
390. [case(AddOrChangeDomain,
391. AddOrChangeGroup,
392. DeleteGroup,
393. RenameGroup,
394. AddOrChangeUser,
395. DeleteUser,
396. RenameUser,
397. ChangeGroupMembership,
398. AddOrChangeAlias,
399. DeleteAlias,
400. RenameAlias,
401. ChangeAliasMembership,
402. DeleteGroupByName,
403. DeleteUserByName )] ULONG Rid;
404. [case(AddOrChangeLsaPolicy,
405. AddOrChangeLsaTDomain,
406. DeleteLsaTDomain,
407. AddOrChangeLsaAccount,
408. DeleteLsaAccount)] PRPC\_SID Sid;
409. [case(AddOrChangeLsaSecret,
410. DeleteLsaSecret)] [string] wchar\_t \* Name;
411. [default] ;
412. } NETLOGON\_DELTA\_ID\_UNION,
413. \*PNETLOGON\_DELTA\_ID\_UNION;
414. typedef struct \_NETLOGON\_DELTA\_ENUM{
415. NETLOGON\_DELTA\_TYPE DeltaType;
416. [switch\_is(DeltaType)] NETLOGON\_DELTA\_ID\_UNION DeltaID;
417. [switch\_is(DeltaType)] NETLOGON\_DELTA\_UNION DeltaUnion;
418. } NETLOGON\_DELTA\_ENUM,
419. \*PNETLOGON\_DELTA\_ENUM;
420. typedef struct \_NETLOGON\_DELTA\_ENUM\_ARRAY{
421. DWORD CountReturned;
422. [size\_is(CountReturned)] PNETLOGON\_DELTA\_ENUM Deltas;
423. } NETLOGON\_DELTA\_ENUM\_ARRAY,
424. \*PNETLOGON\_DELTA\_ENUM\_ARRAY;
425. typedef struct \_NETLOGON\_LOGON\_IDENTITY\_INFO{
426. RPC\_UNICODE\_STRING LogonDomainName;
427. ULONG ParameterControl;
428. OLD\_LARGE\_INTEGER Reserved;
429. RPC\_UNICODE\_STRING UserName;
430. RPC\_UNICODE\_STRING Workstation;
431. } NETLOGON\_LOGON\_IDENTITY\_INFO,
432. \*PNETLOGON\_LOGON\_IDENTITY\_INFO;
433. typedef struct \_NETLOGON\_INTERACTIVE\_INFO{
434. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
435. LM\_OWF\_PASSWORD LmOwfPassword;
436. NT\_OWF\_PASSWORD NtOwfPassword;
437. } NETLOGON\_INTERACTIVE\_INFO,
438. \*PNETLOGON\_INTERACTIVE\_INFO;
439. typedef enum \_NETLOGON\_LOGON\_INFO\_CLASS{
440. NetlogonInteractiveInformation = 1,
441. NetlogonNetworkInformation = 2,
442. NetlogonServiceInformation = 3,
443. NetlogonGenericInformation = 4,
444. NetlogonInteractiveTransitiveInformation = 5,
445. NetlogonNetworkTransitiveInformation = 6,
446. NetlogonServiceTransitiveInformation = 7
447. } NETLOGON\_LOGON\_INFO\_CLASS;
448. typedef struct \_NETLOGON\_SERVICE\_INFO{
449. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
450. LM\_OWF\_PASSWORD LmOwfPassword;
451. NT\_OWF\_PASSWORD NtOwfPassword;
452. } NETLOGON\_SERVICE\_INFO,
453. \*PNETLOGON\_SERVICE\_INFO;
454. typedef struct{
455. CHAR data[8];
456. } LM\_CHALLENGE;
457. typedef struct \_NETLOGON\_NETWORK\_INFO{
458. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
459. LM\_CHALLENGE LmChallenge;
460. STRING NtChallengeResponse;
461. STRING LmChallengeResponse;
462. } NETLOGON\_NETWORK\_INFO,
463. \*PNETLOGON\_NETWORK\_INFO;
464. typedef struct \_NETLOGON\_GENERIC\_INFO{
465. NETLOGON\_LOGON\_IDENTITY\_INFO Identity;
466. RPC\_UNICODE\_STRING PackageName;
467. ULONG DataLength;
468. [size\_is(DataLength)] UCHAR \* LogonData;
469. } NETLOGON\_GENERIC\_INFO,
470. \*PNETLOGON\_GENERIC\_INFO;
471. typedef [switch\_type(NETLOGON\_LOGON\_INFO\_CLASS)] union
472. \_NETLOGON\_LEVEL{
473. [case(NetlogonInteractiveInformation)]
474. PNETLOGON\_INTERACTIVE\_INFO LogonInteractive;
475. [case(NetlogonInteractiveTransitiveInformation)]
476. PNETLOGON\_INTERACTIVE\_INFO LogonInteractiveTransitive;
477. [case(NetlogonServiceInformation)]
478. PNETLOGON\_SERVICE\_INFO LogonService;
479. [case(NetlogonServiceTransitiveInformation)]
480. PNETLOGON\_SERVICE\_INFO LogonServiceTransitive;
481. [case(NetlogonNetworkInformation)]
482. PNETLOGON\_NETWORK\_INFO LogonNetwork;
483. [case(NetlogonNetworkTransitiveInformation)]
484. PNETLOGON\_NETWORK\_INFO LogonNetworkTransitive;
485. [case(NetlogonGenericInformation)]
486. PNETLOGON\_GENERIC\_INFO LogonGeneric;
487. [default]
488. ;
489. } NETLOGON\_LEVEL,
490. \* PNETLOGON\_LEVEL;
491. typedef enum \_NETLOGON\_VALIDATION\_INFO\_CLASS{
492. NetlogonValidationUasInfo = 1,
493. NetlogonValidationSamInfo = 2,
494. NetlogonValidationSamInfo2 = 3,
495. NetlogonValidationGenericInfo = 4,
496. NetlogonValidationGenericInfo2 = 5,
497. NetlogonValidationSamInfo4 = 6
498. } NETLOGON\_VALIDATION\_INFO\_CLASS;
499. typedef struct \_GROUP\_MEMBERSHIP{
500. ULONG RelativeId;
501. ULONG Attributes;
502. } GROUP\_MEMBERSHIP,
503. \*PGROUP\_MEMBERSHIP;
504. typedef struct \_USER\_SESSION\_KEY{
505. CYPHER\_BLOCK data[2];
506. } USER\_SESSION\_KEY,
507. \*PUSER\_SESSION\_KEY;
508. typedef struct \_NETLOGON\_SID\_AND\_ATTRIBUTES{
509. PRPC\_SID Sid;
510. ULONG Attributes;
511. } NETLOGON\_SID\_AND\_ATTRIBUTES,
512. \*PNETLOGON\_SID\_AND\_ATTRIBUTES;
513. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO{
514. OLD\_LARGE\_INTEGER LogonTime;
515. OLD\_LARGE\_INTEGER LogoffTime;
516. OLD\_LARGE\_INTEGER KickOffTime;
517. OLD\_LARGE\_INTEGER PasswordLastSet;
518. OLD\_LARGE\_INTEGER PasswordCanChange;
519. OLD\_LARGE\_INTEGER PasswordMustChange;
520. RPC\_UNICODE\_STRING EffectiveName;
521. RPC\_UNICODE\_STRING FullName;
522. RPC\_UNICODE\_STRING LogonScript;
523. RPC\_UNICODE\_STRING ProfilePath;
524. RPC\_UNICODE\_STRING HomeDirectory;
525. RPC\_UNICODE\_STRING HomeDirectoryDrive;
526. USHORT LogonCount;
527. USHORT BadPasswordCount;
528. ULONG UserId;
529. ULONG PrimaryGroupId;
530. ULONG GroupCount;
531. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
532. ULONG UserFlags;
533. USER\_SESSION\_KEY UserSessionKey;
534. RPC\_UNICODE\_STRING LogonServer;
535. RPC\_UNICODE\_STRING LogonDomainName;
536. PRPC\_SID LogonDomainId;
537. ULONG ExpansionRoom[10];
538. } NETLOGON\_VALIDATION\_SAM\_INFO,
539. \*PNETLOGON\_VALIDATION\_SAM\_INFO;
540. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO2{
541. OLD\_LARGE\_INTEGER LogonTime;
542. OLD\_LARGE\_INTEGER LogoffTime;
543. OLD\_LARGE\_INTEGER KickOffTime;
544. OLD\_LARGE\_INTEGER PasswordLastSet;
545. OLD\_LARGE\_INTEGER PasswordCanChange;
546. OLD\_LARGE\_INTEGER PasswordMustChange;
547. RPC\_UNICODE\_STRING EffectiveName;
548. RPC\_UNICODE\_STRING FullName;
549. RPC\_UNICODE\_STRING LogonScript;
550. RPC\_UNICODE\_STRING ProfilePath;
551. RPC\_UNICODE\_STRING HomeDirectory;
552. RPC\_UNICODE\_STRING HomeDirectoryDrive;
553. USHORT LogonCount;
554. USHORT BadPasswordCount;
555. ULONG UserId;
556. ULONG PrimaryGroupId;
557. ULONG GroupCount;
558. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
559. ULONG UserFlags;
560. USER\_SESSION\_KEY UserSessionKey;
561. RPC\_UNICODE\_STRING LogonServer;
562. RPC\_UNICODE\_STRING LogonDomainName;
563. PRPC\_SID LogonDomainId;
564. ULONG ExpansionRoom[10];
565. ULONG SidCount;
566. [size\_is(SidCount)] PNETLOGON\_SID\_AND\_ATTRIBUTES ExtraSids;
567. } NETLOGON\_VALIDATION\_SAM\_INFO2,
568. \*PNETLOGON\_VALIDATION\_SAM\_INFO2 ;
569. typedef struct \_NETLOGON\_VALIDATION\_GENERIC\_INFO2{
570. ULONG DataLength;
571. [size\_is(DataLength)] UCHAR \* ValidationData;
572. } NETLOGON\_VALIDATION\_GENERIC\_INFO2,
573. \*PNETLOGON\_VALIDATION\_GENERIC\_INFO2;
574. typedef struct \_NETLOGON\_VALIDATION\_SAM\_INFO4 {
575. OLD\_LARGE\_INTEGER LogonTime;
576. OLD\_LARGE\_INTEGER LogoffTime;
577. OLD\_LARGE\_INTEGER KickOffTime;
578. OLD\_LARGE\_INTEGER PasswordLastSet;
579. OLD\_LARGE\_INTEGER PasswordCanChange;
580. OLD\_LARGE\_INTEGER PasswordMustChange;
581. RPC\_UNICODE\_STRING EffectiveName;
582. RPC\_UNICODE\_STRING FullName;
583. RPC\_UNICODE\_STRING LogonScript;
584. RPC\_UNICODE\_STRING ProfilePath;
585. RPC\_UNICODE\_STRING HomeDirectory;
586. RPC\_UNICODE\_STRING HomeDirectoryDrive;
587. unsigned short LogonCount;
588. unsigned short BadPasswordCount;
589. unsigned long UserId;
590. unsigned long PrimaryGroupId;
591. unsigned long GroupCount;
592. [size\_is(GroupCount)] PGROUP\_MEMBERSHIP GroupIds;
593. unsigned long UserFlags;
594. USER\_SESSION\_KEY UserSessionKey;
595. RPC\_UNICODE\_STRING LogonServer;
596. RPC\_UNICODE\_STRING LogonDomainName;
597. PRPC\_SID LogonDomainId;
598. unsigned char LMKey[8];
599. ULONG UserAccountControl;
600. ULONG SubAuthStatus;
601. OLD\_LARGE\_INTEGER LastSuccessfulILogon;
602. OLD\_LARGE\_INTEGER LastFailedILogon;
603. ULONG FailedILogonCount;
604. ULONG Reserved4[1];
605. unsigned long SidCount;
606. [size\_is(SidCount)] PNETLOGON\_SID\_AND\_ATTRIBUTES ExtraSids;
607. RPC\_UNICODE\_STRING DnsLogonDomainName;
608. RPC\_UNICODE\_STRING Upn;
609. RPC\_UNICODE\_STRING ExpansionString1;
610. RPC\_UNICODE\_STRING ExpansionString2;
611. RPC\_UNICODE\_STRING ExpansionString3;
612. RPC\_UNICODE\_STRING ExpansionString4;
613. RPC\_UNICODE\_STRING ExpansionString5;
614. RPC\_UNICODE\_STRING ExpansionString6;
615. RPC\_UNICODE\_STRING ExpansionString7;
616. RPC\_UNICODE\_STRING ExpansionString8;
617. RPC\_UNICODE\_STRING ExpansionString9;
618. RPC\_UNICODE\_STRING ExpansionString10;
619. } NETLOGON\_VALIDATION\_SAM\_INFO4,
620. \*PNETLOGON\_VALIDATION\_SAM\_INFO4;
621. typedef [switch\_type(enum \_NETLOGON\_VALIDATION\_INFO\_CLASS)] union
622. \_NETLOGON\_VALIDATION{
623. [case(NetlogonValidationSamInfo)]
624. PNETLOGON\_VALIDATION\_SAM\_INFO ValidationSam;
625. [case(NetlogonValidationSamInfo2)]
626. PNETLOGON\_VALIDATION\_SAM\_INFO2 ValidationSam2;
627. [case(NetlogonValidationGenericInfo2)]
628. PNETLOGON\_VALIDATION\_GENERIC\_INFO2 ValidationGeneric2;
629. [case(NetlogonValidationSamInfo4)]
630. PNETLOGON\_VALIDATION\_SAM\_INFO4 ValidationSam4;
631. [default]
632. ;
633. } NETLOGON\_VALIDATION,
634. \*PNETLOGON\_VALIDATION;
635. typedef [switch\_type(DWORD)] union
636. \_NETLOGON\_CONTROL\_DATA\_INFORMATION{
637. [case(5,6,9,10)] [string] wchar\_t \* TrustedDomainName;
638. [case(65534)] DWORD DebugFlag;
639. [case(8)] [string] wchar\_t \*UserName;
640. [default]
641. ;
642. } NETLOGON\_CONTROL\_DATA\_INFORMATION,
643. \*PNETLOGON\_CONTROL\_DATA\_INFORMATION;
644. typedef struct \_NETLOGON\_INFO\_1{
645. DWORD netlog1\_flags;
646. NET\_API\_STATUS netlog1\_pdc\_connection\_status;
647. } NETLOGON\_INFO\_1,
648. \*PNETLOGON\_INFO\_1;
649. typedef struct \_NETLOGON\_INFO\_2{
650. DWORD netlog2\_flags;
651. NET\_API\_STATUS netlog2\_pdc\_connection\_status;
652. [string] wchar\_t \* netlog2\_trusted\_dc\_name;
653. NET\_API\_STATUS netlog2\_tc\_connection\_status;
654. } NETLOGON\_INFO\_2,
655. \*PNETLOGON\_INFO\_2;
656. typedef struct \_NETLOGON\_INFO\_3{
657. DWORD netlog3\_flags;
658. DWORD netlog3\_logon\_attempts;
659. DWORD netlog3\_reserved1;
660. DWORD netlog3\_reserved2;
661. DWORD netlog3\_reserved3;
662. DWORD netlog3\_reserved4;
663. DWORD netlog3\_reserved5;
664. } NETLOGON\_INFO\_3,
665. \*PNETLOGON\_INFO\_3;
666. typedef struct \_NETLOGON\_INFO\_4{
667. [string] wchar\_t \* netlog4\_trusted\_dc\_name;
668. [string] wchar\_t \* netlog4\_trusted\_domain\_name;
669. } NETLOGON\_INFO\_4,
670. \*PNETLOGON\_INFO\_4;
671. typedef [switch\_type(DWORD)] union
672. \_NETLOGON\_CONTROL\_QUERY\_INFORMATION{
673. [case(1)] PNETLOGON\_INFO\_1 NetlogonInfo1;
674. [case(2)] PNETLOGON\_INFO\_2 NetlogonInfo2;
675. [case(3)] PNETLOGON\_INFO\_3 NetlogonInfo3;
676. [case(4)] PNETLOGON\_INFO\_4 NetlogonInfo4;
677. [default] ;
678. } NETLOGON\_CONTROL\_QUERY\_INFORMATION,
679. \*PNETLOGON\_CONTROL\_QUERY\_INFORMATION;
680. typedef enum \_SYNC\_STATE{
681. NormalState = 0,
682. DomainState = 1,
683. GroupState = 2,
684. UasBuiltInGroupState = 3,
685. UserState = 4,
686. GroupMemberState = 5,
687. AliasState = 6,
688. AliasMemberState = 7,
689. SamDoneState = 8
690. } SYNC\_STATE,
691. \*PSYNC\_STATE;
692. typedef struct \_DOMAIN\_NAME\_BUFFER{
693. ULONG DomainNameByteCount;
694. [unique, size\_is(DomainNameByteCount)]
695. UCHAR \* DomainNames;
696. } DOMAIN\_NAME\_BUFFER,
697. \*PDOMAIN\_NAME\_BUFFER;
698. typedef struct \_NETLOGON\_LSA\_POLICY\_INFO{
699. ULONG LsaPolicySize;
700. [size\_is(LsaPolicySize)] UCHAR \* LsaPolicy;
701. } NETLOGON\_LSA\_POLICY\_INFO,
702. \*PNETLOGON\_LSA\_POLICY\_INFO;
703. typedef struct \_NETLOGON\_ONE\_DOMAIN\_INFO{
704. RPC\_UNICODE\_STRING DomainName;
705. RPC\_UNICODE\_STRING DnsDomainName;
706. RPC\_UNICODE\_STRING DnsForestName;
707. GUID DomainGuid;
708. PRPC\_SID DomainSid;
709. RPC\_UNICODE\_STRING TrustExtension;
710. RPC\_UNICODE\_STRING DummyString2;
711. RPC\_UNICODE\_STRING DummyString3;
712. RPC\_UNICODE\_STRING DummyString4;
713. ULONG DummyLong1;
714. ULONG DummyLong2;
715. ULONG DummyLong3;
716. ULONG DummyLong4;
717. } NETLOGON\_ONE\_DOMAIN\_INFO,
718. \*PNETLOGON\_ONE\_DOMAIN\_INFO;
719. typedef struct \_NETLOGON\_DOMAIN\_INFO{
720. NETLOGON\_ONE\_DOMAIN\_INFO PrimaryDomain;
721. ULONG TrustedDomainCount;
722. [size\_is(TrustedDomainCount)]
723. PNETLOGON\_ONE\_DOMAIN\_INFO TrustedDomains;
724. NETLOGON\_LSA\_POLICY\_INFO LsaPolicy;
725. RPC\_UNICODE\_STRING DnsHostNameInDs;
726. RPC\_UNICODE\_STRING DummyString2;
727. RPC\_UNICODE\_STRING DummyString3;
728. RPC\_UNICODE\_STRING DummyString4;
729. ULONG WorkstationFlags;
730. ULONG SupportedEncTypes;
731. ULONG DummyLong3;
732. ULONG DummyLong4;
733. } NETLOGON\_DOMAIN\_INFO,
734. \*PNETLOGON\_DOMAIN\_INFO;
735. typedef [switch\_type(DWORD)] union
736. \_NETLOGON\_DOMAIN\_INFORMATION{
737. [case(1)] PNETLOGON\_DOMAIN\_INFO DomainInfo;
738. [case(2)] PNETLOGON\_LSA\_POLICY\_INFO LsaPolicyInfo;
739. } NETLOGON\_DOMAIN\_INFORMATION,
740. \*PNETLOGON\_DOMAIN\_INFORMATION;
741. typedef struct \_NETLOGON\_WORKSTATION\_INFO{
742. NETLOGON\_LSA\_POLICY\_INFO LsaPolicy;
743. [string] wchar\_t \* DnsHostName;
744. [string] wchar\_t \* SiteName;
745. [string] wchar\_t \* Dummy1;
746. [string] wchar\_t \* Dummy2;
747. [string] wchar\_t \* Dummy3;
748. [string] wchar\_t \* Dummy4;
749. RPC\_UNICODE\_STRING OsVersion;
750. RPC\_UNICODE\_STRING OsName;
751. RPC\_UNICODE\_STRING DummyString3;
752. RPC\_UNICODE\_STRING DummyString4;
753. ULONG WorkstationFlags;
754. ULONG KerberosSupportedEncryptionTypes;
755. ULONG DummyLong3;
756. ULONG DummyLong4;
757. } NETLOGON\_WORKSTATION\_INFO,
758. \*PNETLOGON\_WORKSTATION\_INFO;
759. typedef [switch\_type(DWORD)] union
760. \_NETLOGON\_WORKSTATION\_INFORMATION{
761. [case(1)] PNETLOGON\_WORKSTATION\_INFO WorkstationInfo;
762. [case(2)] PNETLOGON\_WORKSTATION\_INFO LsaPolicyInfo;
763. } NETLOGON\_WORKSTATION\_INFORMATION,
764. \*PNETLOGON\_WORKSTATION\_INFORMATION;
765. typedef struct \_NL\_SOCKET\_ADDRESS{
766. [size\_is(iSockaddrLength)] UCHAR \* lpSockaddr;
767. ULONG iSockaddrLength;
768. } NL\_SOCKET\_ADDRESS,
769. \*PNL\_SOCKET\_ADDRESS;
770. typedef struct \_NL\_SITE\_NAME\_ARRAY{
771. ULONG EntryCount;
772. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SiteNames;
773. } NL\_SITE\_NAME\_ARRAY,
774. \*PNL\_SITE\_NAME\_ARRAY;
775. typedef struct \_DS\_DOMAIN\_TRUSTSW{
776. [string] wchar\_t \* NetbiosDomainName;
777. [string] wchar\_t \* DnsDomainName;
778. ULONG Flags;
779. ULONG ParentIndex;
780. ULONG TrustType;
781. ULONG TrustAttributes;
782. PRPC\_SID DomainSid;
783. GUID DomainGuid;
784. } DS\_DOMAIN\_TRUSTSW,
785. \*PDS\_DOMAIN\_TRUSTSW;
786. typedef struct \_NETLOGON\_TRUSTED\_DOMAIN\_ARRAY{
787. DWORD DomainCount;
788. [size\_is(DomainCount)] PDS\_DOMAIN\_TRUSTSW Domains;
789. } NETLOGON\_TRUSTED\_DOMAIN\_ARRAY,
790. \*PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY;
791. typedef struct \_NL\_SITE\_NAME\_EX\_ARRAY{
792. ULONG EntryCount;
793. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SiteNames;
794. [size\_is(EntryCount)] PRPC\_UNICODE\_STRING SubnetNames;
795. } NL\_SITE\_NAME\_EX\_ARRAY,
796. \*PNL\_SITE\_NAME\_EX\_ARRAY;
797. typedef struct \_NL\_GENERIC\_RPC\_DATA{
798. ULONG UlongEntryCount;
799. [size\_is(UlongEntryCount)] ULONG \* UlongData;
800. ULONG UnicodeStringEntryCount;
801. [size\_is(UnicodeStringEntryCount)]
802. PRPC\_UNICODE\_STRING UnicodeStringData;
803. } NL\_GENERIC\_RPC\_DATA,
804. \*PNL\_GENERIC\_RPC\_DATA;
805. typedef struct \_NETLOGON\_VALIDATION\_UAS\_INFO{
806. [string] wchar\_t \* usrlog1\_eff\_name;
807. DWORD usrlog1\_priv;
808. DWORD usrlog1\_auth\_flags;
809. DWORD usrlog1\_num\_logons;
810. DWORD usrlog1\_bad\_pw\_count;
811. DWORD usrlog1\_last\_logon;
812. DWORD usrlog1\_last\_logoff;
813. DWORD usrlog1\_logoff\_time;
814. DWORD usrlog1\_kickoff\_time;
815. DWORD usrlog1\_password\_age;
816. DWORD usrlog1\_pw\_can\_change;
817. DWORD usrlog1\_pw\_must\_change;
818. [string] wchar\_t \* usrlog1\_computer;
819. [string] wchar\_t \* usrlog1\_domain;
820. [string] wchar\_t \* usrlog1\_script\_path;
821. DWORD usrlog1\_reserved1;
822. } NETLOGON\_VALIDATION\_UAS\_INFO,
823. \*PNETLOGON\_VALIDATION\_UAS\_INFO;
824. typedef struct \_NETLOGON\_LOGOFF\_UAS\_INFO{
825. DWORD Duration;
826. USHORT LogonCount;
827. } NETLOGON\_LOGOFF\_UAS\_INFORMATION,
828. \*PNETLOGON\_LOGOFF\_UAS\_INFO;
829. // This structure has been replaced by NETLOGON\_CAPABILITIES.
830. // See the behavior notes associated with the description of
831. // NetrLogonGetCapabilities for details.
832. //typedef [switch\_type(DWORD)] union{
833. // [case(1)] ULONG Dummy;
834. //} NETLOGON\_DUMMY1,
835. // \*PNETLOGON\_DUMMY1;
836. typedef
837. [switch\_type(DWORD)]
838. union \_NETLOGON\_CAPABILITIES {
839. [case(1)]
840. ULONG ServerCapabilities;
841. } NETLOGON\_CAPABILITIES,
842. \*PNETLOGON\_CAPABILITIES;
843. typedef struct \_NETLOGON\_CREDENTIAL{
844. CHAR data[8];
845. } NETLOGON\_CREDENTIAL,
846. \*PNETLOGON\_CREDENTIAL;
847. typedef struct \_NETLOGON\_AUTHENTICATOR{
848. NETLOGON\_CREDENTIAL Credential;
849. DWORD Timestamp;
850. } NETLOGON\_AUTHENTICATOR,
851. \*PNETLOGON\_AUTHENTICATOR;
852. typedef enum \_NETLOGON\_SECURE\_CHANNEL\_TYPE{
853. NullSecureChannel = 0,
854. MsvApSecureChannel = 1,
855. WorkstationSecureChannel = 2,
856. TrustedDnsDomainSecureChannel = 3,
857. TrustedDomainSecureChannel = 4,
858. UasServerSecureChannel = 5,
859. ServerSecureChannel = 6,
860. CdcServerSecureChannel = 7
861. } NETLOGON\_SECURE\_CHANNEL\_TYPE;
862. typedef struct \_UAS\_INFO\_0{
863. CHAR ComputerName[16];
864. ULONG TimeCreated;
865. ULONG SerialNumber;
866. } UAS\_INFO\_0,
867. \*PUAS\_INFO\_0;
868. typedef struct \_DOMAIN\_CONTROLLER\_INFOW{
869. [string,unique] wchar\_t \*DomainControllerName;
870. [string,unique] wchar\_t \*DomainControllerAddress;
871. ULONG DomainControllerAddressType;
872. GUID DomainGuid;
873. [string,unique] wchar\_t \*DomainName;
874. [string,unique] wchar\_t \*DnsForestName;
875. ULONG Flags;
876. [string,unique] wchar\_t \*DcSiteName;
877. [string,unique] wchar\_t \*ClientSiteName;
878. } DOMAIN\_CONTROLLER\_INFOW,
879. \*PDOMAIN\_CONTROLLER\_INFOW;
880. typedef struct \_NL\_TRUST\_PASSWORD{
881. WCHAR Buffer[256];
882. ULONG Length;
883. } NL\_TRUST\_PASSWORD,
884. \*PNL\_TRUST\_PASSWORD;
885. typedef struct \_NL\_PASSWORD\_VERSION{
886. ULONG ReservedField;
887. ULONG PasswordVersionNumber;
888. ULONG PasswordVersionPresent;
889. } NL\_PASSWORD\_VERSION,
890. \*PNL\_PASSWORD\_VERSION;
891. typedef enum \_LSA\_FOREST\_TRUST\_RECORD\_TYPE {
892. ForestTrustTopLevelName = 0,
893. ForestTrustTopLevelNameEx = 1,
894. ForestTrustDomainInfo = 2,
895. } LSA\_FOREST\_TRUST\_RECORD\_TYPE;
896. typedef RPC\_UNICODE\_STRING LSA\_RPC\_UNICODE\_STRING,
897. \*PLSA\_RPC\_UNICODE\_STRING;
898. typedef struct \_LSA\_FOREST\_TRUST\_DOMAIN\_INFO{
899. PRPC\_SID Sid;
900. LSA\_RPC\_UNICODE\_STRING DnsName;
901. LSA\_RPC\_UNICODE\_STRING NetbiosName;
902. } LSA\_FOREST\_TRUST\_DOMAIN\_INFO,
903. \*PLSA\_FOREST\_TRUST\_DOMAIN\_INFO;
904. typedef struct \_LSA\_FOREST\_TRUST\_BINARY\_DATA{
905. [range(0, 131072)] ULONG Length;
906. [size\_is( Length )] UCHAR \* Buffer;
907. } LSA\_FOREST\_TRUST\_BINARY\_DATA,
908. \*PLSA\_FOREST\_TRUST\_BINARY\_DATA;
909. typedef struct \_LSA\_FOREST\_TRUST\_RECORD{
910. ULONG Flags;
911. LSA\_FOREST\_TRUST\_RECORD\_TYPE ForestTrustType;
912. LARGE\_INTEGER Time;
913. [switch\_type( LSA\_FOREST\_TRUST\_RECORD\_TYPE ),
914. switch\_is( ForestTrustType )] union {
915. [case( ForestTrustTopLevelName,
916. ForestTrustTopLevelNameEx )]
917. LSA\_RPC\_UNICODE\_STRING TopLevelName;
918. [case( ForestTrustDomainInfo )]
919. LSA\_FOREST\_TRUST\_DOMAIN\_INFO DomainInfo;
920. [default] LSA\_FOREST\_TRUST\_BINARY\_DATA Data;
921. } ForestTrustData;
922. } LSA\_FOREST\_TRUST\_RECORD,
923. \*PLSA\_FOREST\_TRUST\_RECORD;
924. typedef struct \_LSA\_FOREST\_TRUST\_INFORMATION{
925. [range(0, 4000)] ULONG RecordCount;
926. [size\_is( RecordCount )] PLSA\_FOREST\_TRUST\_RECORD \* Entries;
927. } LSA\_FOREST\_TRUST\_INFORMATION,
928. \*PLSA\_FOREST\_TRUST\_INFORMATION;
929. // Opnum 0
930. NET\_API\_STATUS
931. NetrLogonUasLogon (
932. [in,unique,string] LOGONSRV\_HANDLE ServerName,
933. [in, string] wchar\_t \* UserName,
934. [in, string] wchar\_t \* Workstation,
935. [out] PNETLOGON\_VALIDATION\_UAS\_INFO \*ValidationInformation
936. );
937. // Opnum 1
938. NET\_API\_STATUS
939. NetrLogonUasLogoff (
940. [in,unique,string] LOGONSRV\_HANDLE ServerName,
941. [in, string] wchar\_t \* UserName,
942. [in, string] wchar\_t \* Workstation,
943. [out] PNETLOGON\_LOGOFF\_UAS\_INFO LogoffInformation
944. );
945. // Opnum 2
946. NTSTATUS
947. NetrLogonSamLogon (
948. [in,unique,string] LOGONSRV\_HANDLE LogonServer,
949. [in,string,unique] wchar\_t \* ComputerName,
950. [in,unique] PNETLOGON\_AUTHENTICATOR Authenticator,
951. [in,out,unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
952. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
953. [in,switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
954. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
955. [out,switch\_is(ValidationLevel)]
956. PNETLOGON\_VALIDATION ValidationInformation,
957. [out] UCHAR \* Authoritative
958. );
959. // Opnum 3
960. NTSTATUS
961. NetrLogonSamLogoff (
962. [in,unique,string] LOGONSRV\_HANDLE LogonServer,
963. [in,string,unique] wchar\_t \* ComputerName,
964. [in,unique] PNETLOGON\_AUTHENTICATOR Authenticator,
965. [in,out,unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
966. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
967. [in,switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation
968. );
969. // Opnum 4
970. NTSTATUS
971. NetrServerReqChallenge (
972. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
973. [in, string] wchar\_t \* ComputerName,
974. [in] PNETLOGON\_CREDENTIAL ClientChallenge,
975. [out] PNETLOGON\_CREDENTIAL ServerChallenge
976. );
977. // Opnum 5
978. NTSTATUS
979. NetrServerAuthenticate (
980. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
981. [in,string] wchar\_t \* AccountName,
982. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
983. [in, string] wchar\_t \* ComputerName,
984. [in] PNETLOGON\_CREDENTIAL ClientCredential,
985. [out] PNETLOGON\_CREDENTIAL ServerCredential
986. );
987. // Opnum 6
988. NTSTATUS
989. NetrServerPasswordSet (
990. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
991. [in,string] wchar\_t \* AccountName,
992. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
993. [in, string] wchar\_t \* ComputerName,
994. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
995. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
996. [in] PENCRYPTED\_NT\_OWF\_PASSWORD UasNewPassword
997. );
998. // Opnum 7
999. NTSTATUS
1000. NetrDatabaseDeltas (
1001. [in, string] LOGONSRV\_HANDLE PrimaryName,
1002. [in, string] wchar\_t \* ComputerName,
1003. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1004. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1005. [in] DWORD DatabaseID,
1006. [in, out] PNLPR\_MODIFIED\_COUNT DomainModifiedCount,
1007. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY \*DeltaArray,
1008. [in] DWORD PreferredMaximumLength
1009. );
1010. // Opnum 8
1011. NTSTATUS
1012. NetrDatabaseSync (
1013. [in, string] LOGONSRV\_HANDLE PrimaryName,
1014. [in, string] wchar\_t \* ComputerName,
1015. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1016. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1017. [in] DWORD DatabaseID,
1018. [in, out] ULONG \* SyncContext,
1019. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY \*DeltaArray,
1020. [in] DWORD PreferredMaximumLength
1021. );
1022. // Opnum 9
1023. NTSTATUS
1024. NetrAccountDeltas (
1025. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
1026. [in, string] wchar\_t \* ComputerName,
1027. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1028. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1029. [in] PUAS\_INFO\_0 RecordId,
1030. [in] DWORD Count,
1031. [in] DWORD Level,
1032. [out, size\_is(BufferSize)] UCHAR \* Buffer,
1033. [in] DWORD BufferSize,
1034. [out] ULONG \* CountReturned,
1035. [out] ULONG \* TotalEntries,
1036. [out] PUAS\_INFO\_0 NextRecordId
1037. );
1038. // Opnum 10
1039. NTSTATUS
1040. NetrAccountSync (
1041. [in, unique, string] LOGONSRV\_HANDLE PrimaryName,
1042. [in, string] wchar\_t \* ComputerName,
1043. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1044. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1045. [in] DWORD Reference,
1046. [in] DWORD Level,
1047. [out, size\_is(BufferSize) ] UCHAR \* Buffer,
1048. [in] DWORD BufferSize,
1049. [out] ULONG \* CountReturned,
1050. [out] ULONG \* TotalEntries,
1051. [out] ULONG \* NextReference,
1052. [out] PUAS\_INFO\_0 LastRecordId
1053. );
1054. // Opnum 11
1055. NET\_API\_STATUS
1056. NetrGetDCName (
1057. [in, string] LOGONSRV\_HANDLE ServerName,
1058. [in, unique, string] wchar\_t \*DomainName,
1059. [out, string] wchar\_t \*\*Buffer
1060. );
1061. // Opnum 12
1062. NET\_API\_STATUS
1063. NetrLogonControl(
1064. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1065. [in] DWORD FunctionCode,
1066. [in] DWORD QueryLevel,
1067. [out,switch\_is(QueryLevel)]
1068. PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
1069. );
1070. // Opnum 13
1071. NET\_API\_STATUS
1072. NetrGetAnyDCName (
1073. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1074. [in, unique, string] wchar\_t \*DomainName,
1075. [out, string] wchar\_t \*\*Buffer
1076. );
1077. // Opnum 14
1078. NET\_API\_STATUS
1079. NetrLogonControl2(
1080. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1081. [in] DWORD FunctionCode,
1082. [in] DWORD QueryLevel,
1083. [in,switch\_is(FunctionCode)]
1084. PNETLOGON\_CONTROL\_DATA\_INFORMATION Data,
1085. [out,switch\_is(QueryLevel)]
1086. PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
1087. );
1088. // Opnum 15
1089. NTSTATUS
1090. NetrServerAuthenticate2 (
1091. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
1092. [in,string] wchar\_t \* AccountName,
1093. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
1094. [in, string] wchar\_t \* ComputerName,
1095. [in] PNETLOGON\_CREDENTIAL ClientCredential,
1096. [out] PNETLOGON\_CREDENTIAL ServerCredential,
1097. [in,out] ULONG \* NegotiateFlags
1098. );
1099. // Opnum 16
1100. NTSTATUS
1101. NetrDatabaseSync2 (
1102. [in, string] LOGONSRV\_HANDLE PrimaryName,
1103. [in, string] wchar\_t \* ComputerName,
1104. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1105. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1106. [in] DWORD DatabaseID,
1107. [in] SYNC\_STATE RestartState,
1108. [in, out] ULONG \* SyncContext,
1109. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY \*DeltaArray,
1110. [in] DWORD PreferredMaximumLength
1111. );
1112. // Opnum 17
1113. NTSTATUS
1114. NetrDatabaseRedo(
1115. [in, string] LOGONSRV\_HANDLE PrimaryName,
1116. [in, string] wchar\_t \* ComputerName,
1117. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1118. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1119. [in, size\_is(ChangeLogEntrySize)]
1120. UCHAR \* ChangeLogEntry,
1121. [in] DWORD ChangeLogEntrySize,
1122. [out] PNETLOGON\_DELTA\_ENUM\_ARRAY \*DeltaArray
1123. );
1124. // Opnum 18
1125. NET\_API\_STATUS
1126. NetrLogonControl2Ex(
1127. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1128. [in] DWORD FunctionCode,
1129. [in] DWORD QueryLevel,
1130. [in,switch\_is(FunctionCode)]
1131. PNETLOGON\_CONTROL\_DATA\_INFORMATION Data,
1132. [out,switch\_is(QueryLevel)]
1133. PNETLOGON\_CONTROL\_QUERY\_INFORMATION Buffer
1134. );
1135. // Opnum 19
1136. NTSTATUS
1137. NetrEnumerateTrustedDomains (
1138. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1139. [out] PDOMAIN\_NAME\_BUFFER DomainNameBuffer
1140. );
1141. // Opnum 20
1142. NET\_API\_STATUS
1143. DsrGetDcName(
1144. [in, unique, string ] LOGONSRV\_HANDLE ComputerName,
1145. [in, unique, string] wchar\_t \* DomainName,
1146. [in, unique] GUID \*DomainGuid,
1147. [in, unique] GUID \*SiteGuid,
1148. [in] ULONG Flags,
1149. [out] PDOMAIN\_CONTROLLER\_INFOW \*DomainControllerInfo
1150. );
1151. //This method has been replaced by NetrLogonGetCapabilities.
1152. //See the behavior notes associated with the description of
1153. // NetrLogonGetCapabilities for details.
1154. //NTSTATUS
1155. //NetrLogonDummyRoutine1(
1156. // [in, string] LOGONSRV\_HANDLE ServerName,
1157. // [in, string, unique] wchar\_t\* ComputerName,
1158. // [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1159. // [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1160. // [in] DWORD QueryLevel,
1161. // [out, switch\_is(QueryLevel)] PNETLOGON\_DUMMY1 Buffer
1162. //);
1163. // Opnum 21
1164. NTSTATUS
1165. NetrLogonGetCapabilities(
1166. [in, string] LOGONSRV\_HANDLE ServerName,
1167. [in, string, unique] wchar\_t\* ComputerName,
1168. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1169. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1170. [in] DWORD QueryLevel,
1171. [out, switch\_is(QueryLevel)] PNETLOGON\_CAPABILITIES ServerCapabilities
1172. );
1173. // Opnum 22
1174. NTSTATUS
1175. NetrLogonSetServiceBits(
1176. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1177. [in] DWORD ServiceBitsOfInterest,
1178. [in] DWORD ServiceBits
1179. );
1180. // Opnum 23
1181. NET\_API\_STATUS
1182. NetrLogonGetTrustRid(
1183. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1184. [in,string,unique] wchar\_t \* DomainName,
1185. [out] ULONG \* Rid
1186. );
1187. // Opnum 24
1188. NET\_API\_STATUS
1189. NetrLogonComputeServerDigest(
1190. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1191. [in] ULONG Rid,
1192. [in, size\_is(MessageSize)] UCHAR \* Message,
1193. [in] ULONG MessageSize,
1194. [out] CHAR NewMessageDigest[16],
1195. [out] CHAR OldMessageDigest[16]
1196. );
1197. // Opnum 25
1198. NET\_API\_STATUS
1199. NetrLogonComputeClientDigest(
1200. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1201. [in,string,unique] wchar\_t \* DomainName,
1202. [in, size\_is(MessageSize)] UCHAR \* Message,
1203. [in] ULONG MessageSize,
1204. [out] CHAR NewMessageDigest[16],
1205. [out] CHAR OldMessageDigest[16]
1206. );
1207. // Opnum 26
1208. NTSTATUS
1209. NetrServerAuthenticate3 (
1210. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
1211. [in,string] wchar\_t \* AccountName,
1212. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
1213. [in, string] wchar\_t \* ComputerName,
1214. [in] PNETLOGON\_CREDENTIAL ClientCredential,
1215. [out] PNETLOGON\_CREDENTIAL ServerCredential,
1216. [in,out] ULONG \* NegotiateFlags,
1217. [out] ULONG \* AccountRid
1218. );
1219. // Opnum 27
1220. NET\_API\_STATUS
1221. DsrGetDcNameEx(
1222. [in, unique, string ] LOGONSRV\_HANDLE ComputerName,
1223. [in, unique, string] wchar\_t \* DomainName,
1224. [in, unique] GUID \*DomainGuid,
1225. [in, unique, string] wchar\_t \* SiteName,
1226. [in] ULONG Flags,
1227. [out] PDOMAIN\_CONTROLLER\_INFOW \*DomainControllerInfo
1228. );
1229. // Opnum 28
1230. NET\_API\_STATUS
1231. DsrGetSiteName(
1232. [in, unique, string ] LOGONSRV\_HANDLE ComputerName,
1233. [out, string] wchar\_t \*\*SiteName
1234. );
1235. // Opnum 29
1236. NTSTATUS
1237. NetrLogonGetDomainInfo(
1238. [in, string] LOGONSRV\_HANDLE ServerName,
1239. [in,string,unique] wchar\_t \* ComputerName,
1240. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1241. [in,out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1242. [in] DWORD Level,
1243. [in,switch\_is(Level)] PNETLOGON\_WORKSTATION\_INFORMATION WkstaBuffer,
1244. [out,switch\_is(Level)] PNETLOGON\_DOMAIN\_INFORMATION DomBuffer
1245. );
1246. // Opnum 30
1247. NTSTATUS
1248. NetrServerPasswordSet2 (
1249. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
1250. [in,string] wchar\_t \* AccountName,
1251. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
1252. [in, string] wchar\_t \* ComputerName,
1253. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1254. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1255. [in] PNL\_TRUST\_PASSWORD ClearNewPassword
1256. );
1257. // Opnum 31
1258. NTSTATUS
1259. NetrServerPasswordGet (
1260. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
1261. [in,string] wchar\_t \* AccountName,
1262. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE AccountType,
1263. [in, string] wchar\_t \* ComputerName,
1264. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1265. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1266. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNtOwfPassword
1267. );
1268. // Opnum 32
1269. NTSTATUS
1270. NetrLogonSendToSam (
1271. [in,unique,string] LOGONSRV\_HANDLE PrimaryName,
1272. [in, string] wchar\_t \* ComputerName,
1273. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1274. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1275. [in,size\_is(OpaqueBufferSize)] UCHAR \* OpaqueBuffer,
1276. [in] ULONG OpaqueBufferSize
1277. );
1278. // Opnum 33
1279. NET\_API\_STATUS
1280. DsrAddressToSiteNamesW(
1281. [in,unique,string] LOGONSRV\_HANDLE ComputerName,
1282. [in, range(0,32000)] DWORD EntryCount,
1283. [in,size\_is(EntryCount)] PNL\_SOCKET\_ADDRESS SocketAddresses,
1284. [out] PNL\_SITE\_NAME\_ARRAY \*SiteNames
1285. );
1286. // Opnum 34
1287. NET\_API\_STATUS
1288. DsrGetDcNameEx2(
1289. [in, unique, string ] LOGONSRV\_HANDLE ComputerName,
1290. [in, unique, string] wchar\_t \* AccountName,
1291. [in] ULONG AllowableAccountControlBits,
1292. [in, unique, string] wchar\_t \* DomainName,
1293. [in, unique] GUID \*DomainGuid,
1294. [in, unique, string] wchar\_t \* SiteName,
1295. [in] ULONG Flags,
1296. [out] PDOMAIN\_CONTROLLER\_INFOW \*DomainControllerInfo
1297. );
1298. // Opnum35
1299. NET\_API\_STATUS
1300. NetrLogonGetTimeServiceParentDomain(
1301. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1302. [out, string] wchar\_t \*\*DomainName,
1303. [out] int \* PdcSameSite
1304. );
1305. // Opnum 36
1306. NET\_API\_STATUS
1307. NetrEnumerateTrustedDomainsEx (
1308. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1309. [out] PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY Domains
1310. );
1311. // Opnum 37
1312. NET\_API\_STATUS
1313. DsrAddressToSiteNamesExW(
1314. [in,unique,string] LOGONSRV\_HANDLE ComputerName,
1315. [in, range(0,32000)] DWORD EntryCount,
1316. [in,size\_is(EntryCount)] PNL\_SOCKET\_ADDRESS SocketAddresses,
1317. [out] PNL\_SITE\_NAME\_EX\_ARRAY \*SiteNames
1318. );
1319. // Opnum 38
1320. NET\_API\_STATUS
1321. DsrGetDcSiteCoverageW(
1322. [in,unique,string] LOGONSRV\_HANDLE ServerName,
1323. [out] PNL\_SITE\_NAME\_ARRAY \*SiteNames
1324. );
1325. // Opnum 39
1326. NTSTATUS
1327. NetrLogonSamLogonEx (
1328. [in] handle\_t ContextHandle,
1329. [in,unique,string] wchar\_t \* LogonServer,
1330. [in,unique,string] wchar\_t \* ComputerName,
1331. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
1332. [in,switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
1333. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
1334. [out,switch\_is(ValidationLevel)]
1335. PNETLOGON\_VALIDATION ValidationInformation,
1336. [out] UCHAR \* Authoritative,
1337. [in,out] ULONG \* ExtraFlags
1338. );
1339. // Opnum 40
1340. NET\_API\_STATUS
1341. DsrEnumerateDomainTrusts (
1342. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1343. [in] ULONG Flags,
1344. [out] PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY Domains
1345. );
1346. // Opnum 41
1347. NET\_API\_STATUS
1348. DsrDeregisterDnsHostRecords (
1349. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1350. [in, unique, string] wchar\_t \* DnsDomainName,
1351. [in, unique] GUID \*DomainGuid,
1352. [in, unique] GUID \*DsaGuid,
1353. [in, string] wchar\_t \* DnsHostName
1354. );
1355. // Opnum 42
1356. NTSTATUS
1357. NetrServerTrustPasswordsGet (
1358. [in,unique,string] LOGONSRV\_HANDLE TrustedDcName,
1359. [in,string] wchar\_t \* AccountName,
1360. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
1361. [in, string] wchar\_t \* ComputerName,
1362. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1363. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1364. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNewOwfPassword,
1365. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedOldOwfPassword
1366. );
1367. // Opnum 43
1368. NET\_API\_STATUS
1369. DsrGetForestTrustInformation (
1370. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1371. [in, unique, string] wchar\_t \* TrustedDomainName,
1372. [in] DWORD Flags,
1373. [out] PLSA\_FOREST\_TRUST\_INFORMATION \* ForestTrustInfo
1374. );
1375. // Opnum 44
1376. NTSTATUS
1377. NetrGetForestTrustInformation (
1378. [in,unique,string] LOGONSRV\_HANDLE ServerName,
1379. [in, string] wchar\_t \* ComputerName,
1380. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1381. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1382. [in] DWORD Flags,
1383. [out] PLSA\_FOREST\_TRUST\_INFORMATION \* ForestTrustInfo
1384. );
1385. // Opnum 45
1386. NTSTATUS
1387. NetrLogonSamLogonWithFlags (
1388. [in,unique,string] LOGONSRV\_HANDLE LogonServer,
1389. [in,string,unique] wchar\_t \* ComputerName,
1390. [in,unique] PNETLOGON\_AUTHENTICATOR Authenticator,
1391. [in,out,unique] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1392. [in] NETLOGON\_LOGON\_INFO\_CLASS LogonLevel,
1393. [in,switch\_is(LogonLevel)] PNETLOGON\_LEVEL LogonInformation,
1394. [in] NETLOGON\_VALIDATION\_INFO\_CLASS ValidationLevel,
1395. [out,switch\_is(ValidationLevel)]
1396. PNETLOGON\_VALIDATION ValidationInformation,
1397. [out] UCHAR \* Authoritative,
1398. [in,out] ULONG \* ExtraFlags
1399. );
1400. // Opnum 46
1401. NTSTATUS
1402. NetrServerGetTrustInfo (
1403. [in,unique,string] LOGONSRV\_HANDLE TrustedDcName,
1404. [in,string] wchar\_t \* AccountName,
1405. [in] NETLOGON\_SECURE\_CHANNEL\_TYPE SecureChannelType,
1406. [in, string] wchar\_t \* ComputerName,
1407. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1408. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1409. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedNewOwfPassword,
1410. [out] PENCRYPTED\_NT\_OWF\_PASSWORD EncryptedOldOwfPassword,
1411. [out] PNL\_GENERIC\_RPC\_DATA \*TrustInfo
1412. );
1413. // Opnum 47
1414. //Local only method
1415. NTSTATUS
1416. OpnumUnused47 (
1417. void
1418. );
1419. typedef struct \_NL\_DNS\_NAME\_INFO{
1420. ULONG Type;
1421. [string] wchar\_t \* DnsDomainInfo;
1422. ULONG DnsDomainInfoType;
1423. ULONG Priority;
1424. ULONG Weight;
1425. ULONG Port;
1426. UCHAR Register;
1427. ULONG Status;
1428. } NL\_DNS\_NAME\_INFO,
1429. \*PNL\_DNS\_NAME\_INFO;
1430. typedef struct \_NL\_DNS\_NAME\_INFO\_ARRAY{
1431. ULONG EntryCount;
1432. [size\_is(EntryCount)] PNL\_DNS\_NAME\_INFO DnsNamesInfo;
1433. } NL\_DNS\_NAME\_INFO\_ARRAY,
1434. \*PNL\_DNS\_NAME\_INFO\_ARRAY;
1435. // Opnum 48
1436. NTSTATUS
1437. DsrUpdateReadOnlyServerDnsRecords (
1438. [in, unique, string] LOGONSRV\_HANDLE ServerName,
1439. [in, string] wchar\_t \* ComputerName,
1440. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
1441. [out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1442. [in, unique, string] wchar\_t \* SiteName,
1443. [in] ULONG DnsTtl,
1444. [in, out] PNL\_DNS\_NAME\_INFO\_ARRAY DnsNames
1445. );
1447. typedef struct \_NL\_OSVERSIONINFO\_V1{
1448. DWORD dwOSVersionInfoSize;
1449. DWORD dwMajorVersion;
1450. DWORD dwMinorVersion;
1451. DWORD dwBuildNumber;
1452. DWORD dwPlatformId;
1453. wchar\_t szCSDVersion[128];
1454. USHORT wServicePackMajor;
1455. USHORT wServicePackMinor;
1456. USHORT wSuiteMask;
1457. UCHAR wProductType;
1458. UCHAR wReserved;
1459. } NL\_OSVERSIONINFO\_V1;
1460. typedef struct \_NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1{
1461. [unique,string] wchar\_t \* ClientDnsHostName;
1462. [unique] NL\_OSVERSIONINFO\_V1 \*OsVersionInfo\_V1;
1463. [unique,string] wchar\_t \* OsName;
1464. } NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1;
1465. typedef [switch\_type(DWORD)] union{
1466. [case(1)] NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 V1;
1467. } NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES;
1468. typedef struct \_NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1{
1469. [unique,string] wchar\_t \*HubName;
1470. [unique,string] wchar\_t \*\*OldDnsHostName;
1471. [unique] ULONG \* SupportedEncTypes;
1472. } NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1;
1473. typedef [switch\_type(DWORD)] union{
1474. [case(1)] NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 V1;
1475. } NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES;
1476. // Opnum 49
1477. NTSTATUS
1478. NetrChainSetClientAttributes(
1479. [in,string,ref] LOGONSRV\_HANDLE PrimaryName,
1480. [in,string,ref] wchar\_t \* ChainedFromServerName,
1481. [in,string,ref] wchar\_t \* ChainedForClientName,
1482. [in,ref] PNETLOGON\_AUTHENTICATOR Authenticator,
1483. [in,out,ref] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
1484. [in] DWORD dwInVersion,
1485. [in,ref] [switch\_is(dwInVersion)]
1486. NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES \*pmsgIn,
1487. [in,out,ref] DWORD \* pdwOutVersion,
1488. [in,out,ref] [switch\_is(\*pdwOutVersion)]
1489. NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES \*pmsgOut
1490. );
1491. }

# Appendix B: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

* Windows NT operating system
* Windows 2000 operating system
* Windows XP operating system
* Windows Server 2003 operating system
* Windows Vista operating system
* Windows Server 2008 operating system
* Windows 7 operating system
* Windows Server 2008 R2 operating system
* Windows 8 operating system
* Windows Server 2012 operating system
* Windows 8.1 operating system
* Windows Server 2012 R2 operating system
* Windows 10 operating system
* Windows Server 2016 operating system
* Windows Server operating system

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

[<1> Section 1.3.3](#Appendix_A_Target_1): Sharing the user account database is achieved in Windows via replication of the account [**database**](#gt_00f35ba3-4dbb-4ff9-8e27-572a6aea1b15) among [**DCs**](#gt_76a05049-3531-4abd-aec8-30e19954b4bd) so that each DC in the [**domain**](#gt_b0276eb2-4e65-4cf1-a718-e0920a614aca) has the same copy of the database. On Windows DCs, replication is performed by the [**Active Directory**](#gt_e467d927-17bf-49c9-98d1-96ddf61ddd90) replication service (see [[MS-DRSR]](%5bMS-DRSR%5d.pdf#Section_f977faaa673e4f66b9bf48c640241d47)), except on Windows NT 4.0 operating system DCs, where replication is performed by the Netlogon replication.

[<2> Section 1.3.3](#Appendix_A_Target_2): Except for DCs running Windows NT 4.0, synchronization between DCs running Windows is performed by the Active Directory replication service [MS-DRSR]. Synchronization involving a DC running Windows NT 4.0 is performed by the Netlogon service.

[<3> Section 1.3.3](#Appendix_A_Target_3): In Windows NT 4.0, a single DC in a domain is designated the [**primary domain controller (PDC)**](#gt_663cb13a-8b75-477f-b6e1-bea8f2fba64d). The PDC is the only DC that accepts changes to the account information it stores. A Windows NT 4.0 domain has zero or more [**backup domain controllers (BDCs)**](#gt_ce1138c6-7ab4-4c37-98b4-95599071c3c3).

[<4> Section 1.3.3](#Appendix_A_Target_4): Netlogon replication requires the PDC to run Windows NT Server 4.0 operating system, Windows 2000 Server operating system, or Windows Server 2003, while BDCs run Windows NT Server 4.0. Windows Server 2008 does not support replication to Windows NT 4.0 BDCs.

[<5> Section 1.3.8.1](#Appendix_A_Target_5): Microsoft's first major entrance into the network operating system field was LAN Manager. While LAN Manager produced many of the underlying paradigms for how services are accessed over the network, the implementation of those paradigms changed significantly between LAN Manager and Windows NT. In cases where those interfaces were implemented by using [**RPC**](#gt_8a7f6700-8311-45bc-af10-82e10accd331) [[MS-RPCE]](%5bMS-RPCE%5d.pdf#Section_290c38b192fe422991e64fc376610c15), Windows NT could have had support for older clients to make use of those interfaces or methods within those interfaces. However, Windows NT–based products do not use those methods; therefore, those methods are not documented.

[<6> Section 1.6](#Appendix_A_Target_6): The Netlogon Remote Protocol is used only when the client or server is a member of a Windows domain.

[<7> Section 2.2.1.1.2](#Appendix_A_Target_7): The value of **MaximumLength** is ignored by the Windows NT 4.0 implementation.

[<8> Section 2.2.1.2.1](#Appendix_A_Target_8): The DOMAIN\_CONTROLLER\_INFOW structure is not supported in Windows NT.

[<9> Section 2.2.1.2.1](#Appendix_A_Target_9): IPv6 is not supported in Windows NT, Windows 2000, Windows XP, or Windows Server 2003.

[<10> Section 2.2.1.2.1](#Appendix_A_Target_10): In Windows NT, Windows 2000 Server, Windows XP, and Windows Server 2003, this address is an IPv4 address. For all other Windows releases, this address can be an IPv4 or IPv6 address.

[<11> Section 2.2.1.2.1](#Appendix_A_Target_11): Windows NT-based domain controllers do not have a domain [**GUID**](#gt_f49694cc-c350-462d-ab8e-816f0103c6c1).

[<12> Section 2.2.1.2.1](#Appendix_A_Target_12): **[read-only domain controllers (RODCs)](#gt_8b0a073b-3099-4efe-8b81-c2886b66a870)** are not supported in Windows NT Server operating system, Windows 2000 Server and Windows Server 2003.

[<13> Section 2.2.1.2.1](#Appendix_A_Target_13): **[Writable domain controller](#gt_9d964ddb-09d6-4a1b-b27b-42adabc07993)**s are not supported in Windows NT Server, Windows 2000, and Windows Server 2003. The concept of designating a DC as writable was added when read-only DCs were created.

[<14> Section 2.2.1.2.1](#Appendix_A_Target_14): Active Directory Web Service is not available in Windows NT and Windows 2000. It is available in Windows Server 2003 and Windows Server 2008 when Active Directory Management Gateway Service is installed.

[<15> Section 2.2.1.2.1](#Appendix_A_Target_15): Windows NT-based domain controllers do not have an associated [**site**](#gt_8abdc986-5679-42d9-ad76-b11eb5a0daba).

[<16> Section 2.2.1.2.5](#Appendix_A_Target_16): The **Status** field is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<17> Section 2.2.1.2.6](#Appendix_A_Target_17): **DnsNamesInfo** is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<18> Section 2.2.1.3.3](#Appendix_A_Target_18): The NL\_AUTH\_SHA2\_SIGNATURE structure is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista.

[<19> Section 2.2.1.3.6](#Appendix_A_Target_19): The NETLOGON\_WORKSTATION\_INFO structure is not supported in Windows NT.

[<20> Section 2.2.1.3.6](#Appendix_A_Target_20): For example, for Windows 7 Ultimate operating system, the string "Windows 7 Ultimate" is used.

[<21> Section 2.2.1.3.6](#Appendix_A_Target_21): The **KerberosSupportedEncryptionTypes** field is not supported in Windows NT, Windows 2000, and Windows Server 2003.

[<22> Section 2.2.1.3.7](#Appendix_A_Target_22): The **NL\_TRUST\_PASSWORD** structure is not supported in Windows NT.

[<23> Section 2.2.1.3.8](#Appendix_A_Target_23): The **NL\_PASSWORD\_VERSION** structure is not supported in Windows NT.

[<24> Section 2.2.1.3.9](#Appendix_A_Target_24): The **NETLOGON\_WORKSTATION\_INFORMATION** union is not supported in Windows NT.

[<25> Section 2.2.1.3.10](#Appendix_A_Target_25): The **NETLOGON\_ONE\_DOMAIN\_INFO** structure is not supported in Windows NT.

[<26> Section 2.2.1.3.11](#Appendix_A_Target_26): The **NETLOGON\_DOMAIN\_INFO** structure is not supported in Windows NT.

[<27> Section 2.2.1.3.11](#Appendix_A_Target_27): Windows NT, Windows 2000, and Windows XP ignore the **SupportedEncTypes** field.

[<28> Section 2.2.1.3.12](#Appendix_A_Target_28): The **NETLOGON\_DOMAIN\_INFORMATION** structure is not implemented in Windows NT.

[<29> Section 2.2.1.3.13](#Appendix_A_Target_29): One or both domains in a [**secure channel**](#gt_08ce423c-9f9c-48ed-afa8-8b64c04ecdca) is required to be a Windows NT 4.0 domain.

[<30> Section 2.2.1.3.13](#Appendix_A_Target_30): The **CdcServerSecureChannel** type is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<31> Section 2.2.1.3.14](#Appendix_A_Target_31): The **NETLOGON\_CAPABILITIES** union is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<32> Section 2.2.1.3.15](#Appendix_A_Target_32): The normal (writable) DC cannot be a Windows Server 2003 or a Windows 2000 Server DC.

[<33> Section 2.2.1.3.15](#Appendix_A_Target_33): The following table defines the **dwMajorVersion** values.

| Value | Meaning |
| --- | --- |
| 4 | The operating system is Windows NT 4.0. |
| 5 | The operating system is Windows 2000, Windows XP, Windows Server 2003, or Windows Server 2003 R2 operating system. |
| 6 | The operating system is Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, or Windows Server 2012 R2. |
| 10 | The operating system is Windows 10, Windows Server 2016, or Windows Server operating system. |

[<34> Section 2.2.1.3.15](#Appendix_A_Target_34): The following table defines the **dwMinorVersion** values.

| Value | Meaning |
| --- | --- |
| 0 | The operating system is Windows NT 4.0, Windows 2000, Windows Vista, Windows Server 2008, Windows 10, Windows Server 2016, or Windows Server operating system. |
| 1 | The operating system is Windows XP, Windows 7, or Windows Server 2008 R2. |
| 2 | The operating system is Windows XP Professional x64 Edition operating system, Windows Server 2003, Windows Server 2003 R2, Windows 8, or Windows Server 2012. |
| 3 | The operating system is Windows 8.1 or Windows Server 2012 R2. |

[<35> Section 2.2.1.3.15](#Appendix_A_Target_35): VER\_NT\_WORKSTATION identifies the operating system as one of the following: Windows NT Workstation 4.0 operating system, Windows 2000 Professional operating system, Windows XP Home Edition operating system, Windows XP Professional operating system, Windows Vista, Windows 7, Windows 8, Windows 8.1, or Windows 10.

[<36> Section 2.2.1.3.15](#Appendix_A_Target_36): The **wReserved** field is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. The Netlogon server ignores this value.

[<37> Section 2.2.1.3.16](#Appendix_A_Target_37): The normal (writable) DC cannot be a Windows 2000 Server or a Windows Server 2003 domain controller.

[<38> Section 2.2.1.3.16](#Appendix_A_Target_38): The **OsName** field is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<39> Section 2.2.1.3.17](#Appendix_A_Target_39): Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista do not support V1.

[<40> Section 2.2.1.3.18](#Appendix_A_Target_40): The normal (writable) DC cannot be a Windows 2000 Server or a Windows Server 2003 DC.

[<41> Section 2.2.1.3.18](#Appendix_A_Target_41): RODCs are not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

[<42> Section 2.2.1.3.18](#Appendix_A_Target_42): The **SupportedEncTypes** field is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<43> Section 2.2.1.3.19](#Appendix_A_Target_43): The **V1** field is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<44> Section 2.2.1.4.16](#Appendix_A_Target_44): The NETLOGON\_LOGON\_INFO\_CLASS enumeration types are not supported in Windows Vista.

[<45> Section 2.2.1.4.17](#Appendix_A_Target_45): The NETLOGON\_VALIDATION\_INFO\_CLASS enumeration types are not supported in Windows Vista.

[<46> Section 2.2.1.4.17](#Appendix_A_Target_46): Except in Windows Vista, the NETLOGON\_VALIDATION\_INFO\_CLASS enumeration has **NetlogonValidationUasInfo** type defined. This value is used by LAN Manager in support of LAN Manager products, and is beyond the scope of this document.

[<47> Section 2.2.1.5.1](#Appendix_A_Target_47): The recipient of the message waits for the indicated number of seconds before contacting the sender.

[<48> Section 2.2.1.5.22](#Appendix_A_Target_48): Except for Windows NT, **NumControllerEntries** is set to zero in the NETLOGON\_DELTA\_TRUSTED\_DOMAINS structure.

[<49> Section 2.2.1.5.22](#Appendix_A_Target_49): Except for Windows NT, **ControllerNames** is set to NULL in the NETLOGON\_DELTA\_TRUSTED\_DOMAINS structure.

[<50> Section 2.2.1.5.28](#Appendix_A_Target_50): In Windows NT 4.0 replication, the **DeleteGroupByName**, **DeleteUserByName**, and **SerialNumberSkip** types require NegotiateFlags=0x00000010. For more information, see the Capability Negotiation bullet in section [1.7](#Section_b5ad98b323be467e91cda580aab8abaf) and the *NegotiateFlags* parameter description in sections [3.5.4.4.3](#Section_985982ae9aa84565b30b33d6353d3355) (NetrServerAuthenticate2) and [3.5.4.4.2](#Section_3a9ed16f801445ae80afc0ecb06e2db9) (NetrServerAuthenticate3).

[<51> Section 2.2.1.6.2](#Appendix_A_Target_51): **DS\_DOMAIN\_TRUSTSW** structure is not supported in Windows NT.

[<52> Section 2.2.1.6.2](#Appendix_A_Target_52): 0x00000001 is supported only in Windows NT.

[<53> Section 2.2.1.6.2](#Appendix_A_Target_53): Trust with an Active Directory domain is not supported in Windows NT.

[<54> Section 2.2.1.6.2](#Appendix_A_Target_54): A trust link is valid only for Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 domains.

[<55> Section 2.2.1.6.3](#Appendix_A_Target_55): The **NETLOGON\_TRUSTED\_DOMAIN\_ARRAY** structure is not supported in Windows NT.

[<56> Section 2.2.1.6.4](#Appendix_A_Target_56): The **NL\_GENERIC\_RPC\_DATA** structure is not supported in Windows NT or Windows 2000.

[<57> Section 2.2.1.7.2](#Appendix_A_Target_57): The **NETLOGON\_INFO\_1** structure contains information about the state of the database synchronization for Windows NT 4.0 backup domain controllers only.

[<58> Section 2.2.1.7.2](#Appendix_A_Target_58): Flags A, B, C, and D are set only in the query response from a Windows NT 4.0-based backup domain controller. Flags E, F, and G are not available in Windows NT and cannot be set in the query response from a domain controller running Windows NT.

[<59> Section 2.2.1.7.3](#Appendix_A_Target_59): Flags A, B, and C cannot be set in the query response from a server running Windows NT. Flag C is also not supported in Windows 2000 or Windows XP.

[<60> Section 2.2.1.8](#Appendix_A_Target_60): The unsupported structures are used in Windows releases that are not applicable to this specification.

[<61> Section 2.2.1.8.4](#Appendix_A_Target_61): Windows never uses the NETLOGON\_DUMMY1 union.

[<62> Section 3](#Appendix_A_Target_62): In Windows NT 4.0, the Netlogon Remote Protocol RPC interface is used to replicate account information from the primary domain controllers (PDCs) to the backup domain controllers (BDCs). PDCs also use [**mailslots**](#gt_f53fe4b9-8e1d-4366-9254-3c4f73269e78) to broadcast messages to the BDCs; these messages (as specified in section [2.2.1.5.1](#Section_b3a7e5f3d6694f54acb8e85580eaf46d)) are not transmitted via RPC.

[<63> Section 3](#Appendix_A_Target_63): Except in Windows NT, the server defaults to the [**primary domain**](#gt_387021de-3d6b-4372-835f-0d68c50cb496) if the name is not found.

[<64> Section 3.1.1](#Appendix_A_Target_64): In all applicable Windows Server releases except Windows NT, for computer accounts in a domain, the [**OWF**](#gt_9a5d11c7-eea9-4217-b9a8-478c6786e9e8) of the [**shared secret**](#gt_ae8614db-83d9-406d-aa79-90b2f07c3ed1) is stored in the **unicodePwd** attribute of the computer account object in Active Directory ([[MS-ADTS]](%5bMS-ADTS%5d.pdf#Section_d243592709994c628c6d13ba31a52e1a) section 6.4.2).

For [**trusts**](#gt_5ee032d0-d944-4acb-bbb5-b1cfc7df6db6) with applicable Windows Server releases domains (except Windows NT), the shared secret is stored in the **trustAuthIncoming** attribute ([MS-ADTS] section 6.1.6.7.10) and the **trustAuthOutgoing** attribute ([MS-ADTS] section 6.1.6.7.11) of the [**trusted domain object (TDO)**](#gt_f2ceef4e-999b-4276-84cd-2e2829de5fc4) that contains trust information in Active Directory ([MS-ADTS] section 6.1.6.9.1). Depending on the **AuthType** either the shared secret (TRUST\_AUTH\_TYPE\_CLEAR) or NTOWFv1 (TRUST\_AUTH\_TYPE\_NT4OWF) is stored.

For trusts with Windows NT 4.0 domains, the OWF of the shared secret is stored in the **trustAuth** attribute of the corresponding TDO for the Windows NT 4.0 domain.

[<65> Section 3.1.1](#Appendix_A_Target_65): In Windows NT 4.0 ([[MS-SAMR]](%5bMS-SAMR%5d.pdf#Section_4df07fab1bbc452f8e927853a3c7e380) section 3.1.1.3), the OWF of the shared secret is stored as an attribute of the computer account object (for [**domain members**](#gt_6234a38c-ed1b-4c69-969f-6e6479566f65)) or the interdomain trust account object (for domain trusts).

[<66> Section 3.1.1](#Appendix_A_Target_66): Windows uses the Netlogon Remote Protocol to change the machine account password every 30 days by default. The value is configurable with a minimum of one day and maximum of 1,000,000 days.

[<67> Section 3.1.1](#Appendix_A_Target_67): In all applicable Windows Server releases (except Windows NT), the trust password version is stored in the TRUST\_AUTH\_TYPE\_VERSION of the **trustAuthIncoming** attribute ([MS-ADTS] section 6.1.6.7.10) and the **trustAuthOutgoing** attribute ([MS-ADTS] section 6.1.6.7.11) of the TDO that contains trust information in Active Directory ([MS-ADTS] section 6.1.6.9.1). The trust password version is not maintained for Windows NT 4.0 domains.

[<68> Section 3.1.1](#Appendix_A_Target_68): The following Windows registry settings are used to persistently store and retrieve the SealSecureChannel variable:

* RegistryValueName: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueType: 4
* RegistryValue: SealSecureChannel

[<69> Section 3.1.4.1](#Appendix_A_Target_69): Returning the negotiated flags for the current exchange is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<70> Section 3.1.4.1](#Appendix_A_Target_70): Comparing the received ServerCapabilities with the negotiated NegotiateFlags is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<71> Section 3.1.4.2](#Appendix_A_Target_71): The negotiable options J through S are not supported in Windows NT. Option T is not supported in Windows NT or Windows 2000.

[<72> Section 3.1.4.2](#Appendix_A_Target_72): This flag is used in Windows NT 3.5 operating system only.

[<73> Section 3.1.4.2](#Appendix_A_Target_73): The negotiable option U is supported in Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

[<74> Section 3.1.4.2](#Appendix_A_Target_74): The negotiable option V is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

[<75> Section 3.1.4.2](#Appendix_A_Target_75): The negotiable option W is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<76> Section 3.1.4.2](#Appendix_A_Target_76): The negotiable option Y is not supported in Windows NT prior to Windows NT 4.0 operating system Service Pack 2 (SP2).

[<77> Section 3.1.4.6](#Appendix_A_Target_77): For Windows, the client binds to the RPC server using TCP (except for Windows NT, in which the client binds to the RPC server using named pipes). If RPC returns an error indicating that the protocol sequence is not supported, then the client binds to the RPC server using named pipes.

[<78> Section 3.1.4.6](#Appendix_A_Target_78): Windows NT 4.0 operating system Service Pack 4 (SP4) does not support Secure RPC and does not perform a secure bind.

[<79> Section 3.1.4.6](#Appendix_A_Target_79): Windows caches and reuses the binding for subsequent RPC calls to the server.

[<80> Section 3.1.6](#Appendix_A_Target_80): When Netlogon receives a PolicyChange event, NRPC implementations that use the Windows registry to persistently store and retrieve the SealSecureChannel variable need to load the new value from the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters registry path and SealSecureChannel key.

[<81> Section 3.3](#Appendix_A_Target_81): The Windows Netlogon SSP is not provided for use by other applications. It has neither the full functionally of public [**SSPs**](#gt_e0edad22-1b0e-42f3-8e51-50f8aa30b29a) nor access from non-[**LSA**](#gt_9e5f2104-d6df-4ae7-8a5c-6bd14a0da8fa) applications.

[<82> Section 3.3](#Appendix_A_Target_82): The Netlogon capability of encrypting and signing data during communication is not supported in Windows NT prior to Windows NT 4.0 operating system Service Pack 6 (SP6).

[<83> Section 3.3.4.2.2](#Appendix_A_Target_83): Windows disregards the **Flags** data.

[<84> Section 3.4](#Appendix_A_Target_84): Netlogon runs only on machines joined to a domain ([MS-ADTS] section 6.4). Upon startup, it locates a domain controller and establishes a secure channel to it. It is used for secure communication between the client and the domain controller and for passing sensitive data between the two entities. Except in Windows NT, Netlogon also registers the [**service principal names (SPNs)**](#gt_547217ca-134f-4b43-b375-f5bca4c16ce4) for the computer that it runs on. It registers the SPNs of the form "HOST/NetBIOSName" and "HOST/Full.Dns.Name", which updates the **servicePrincipalName** attribute of the computer account object in Active Directory.

[<85> Section 3.4.1](#Appendix_A_Target_85): **RejectMD5Servers** is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

The Windows registry settings used to persistently store and retrieve the RejectMD5Servers variable are the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and RejectMD5Servers key.

[<86> Section 3.4.1](#Appendix_A_Target_86): The following Windows registry settings are used to persistently store and retrieve the **RequireSignOrSeal** variable:

* RegistryValueName: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueType: 4
* RegistryValue: RequireSignOrSeal

See [[MS-GPSB]](%5bMS-GPSB%5d.pdf#Section_6a07a06be62847659d910d63ba47fdc0) section 2.2.5 for information on setting registry entries.

[<87> Section 3.4.1](#Appendix_A_Target_87): **RequireStrongKey** is not supported in Windows NT.

[<88> Section 3.4.1](#Appendix_A_Target_88): The Windows registry settings used to persistently store and retrieve the **RequireStrongKey** variable are as follows:

* RegistryValueName: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueType: 4
* RegistryValue: RequireStrongKey

[<89> Section 3.4.3](#Appendix_A_Target_89): Windows uses 4096. Other implementations can use any value.

[<90> Section 3.4.3](#Appendix_A_Target_90): Implementations that use the Windows registry to persistently store and retrieve the settings for **ClientCapabilities** bit **O** use the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and the **SignSecureChannel** and **SealSecureChannel** values to indicate whether bit **O** should be set. If either of these registry values are set to 0x1, then bit **O** is set.

Implementations that use the Windows registry to persistently store settings for **ClientCapabilities** bit **U** use the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and NeutralizeNt4Emulator key to indicate whether bit **U** is set. If this registry value is set to 0x1, then bit **U** is set.

[<91> Section 3.4.3](#Appendix_A_Target_91): Windows NT 4.0 SP4, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 initialize **RequireSignOrSeal** to FALSE.

[<92> Section 3.4.3](#Appendix_A_Target_92): Windows initializes **RequireStrongKey** to FALSE.

[<93> Section 3.4.5.1.3](#Appendix_A_Target_93): All applications available as part of Windows set the *SiteGuid* parameter to NULL.

[<94> Section 3.4.5.1.11](#Appendix_A_Target_94): The *ServerName* is a normal (writable) DC, but is not a Windows Server 2003 or a Windows 2000 Server DC.

[<95> Section 3.4.5.1.11](#Appendix_A_Target_95): The client has to be an RODC.

[<96> Section 3.4.5.2.4](#Appendix_A_Target_96): The NetrServerAuthenticate method is used only in Windows NT Server 3.1 operating system.

[<97> Section 3.4.5.2.5](#Appendix_A_Target_97): Windows clients re-establish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<98> Section 3.4.5.2.6](#Appendix_A_Target_98): Windows clients re-establish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<99> Section 3.4.5.2.7](#Appendix_A_Target_99): Windows clients re-establish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<100> Section 3.4.5.2.9](#Appendix_A_Target_100): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<101> Section 3.4.5.2.10](#Appendix_A_Target_101): NetrLogonGetCapabilities is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008 clients.

[<102> Section 3.4.5.2.10](#Appendix_A_Target_102): Re-establishing the secure channel with the DC is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<103> Section 3.4.5.2.10](#Appendix_A_Target_103): For Windows DCs, the STATUS\_NOT\_IMPLEMENTED error means the DC is a Windows NT, Windows Server 2003, or Windows Server 2008 machine.

[<104> Section 3.4.5.2.10](#Appendix_A_Target_104): Windows clients re-establish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<105> Section 3.4.5.2.11](#Appendix_A_Target_105): The normal (writable) DC cannot be a Windows 2000 Server or a Windows Server 2003 DC.

[<106> Section 3.4.5.3.2](#Appendix_A_Target_106): Except in Windows NT 3.1 operating system, Windows encrypts by using the negotiated encryption algorithm and the [**session key**](#gt_4f67a585-fb00-4166-93e8-cf4abca8226d).

For Windows NT 3.1, encrypt as follows.

1. InitLMKey(KeyIn, KeyOut)
2. KeyOut[0] = KeyIn[0] >> 0x01;
3. KeyOut[1] = ((KeyIn[0]&0x01)<<6) | (KeyIn[1]>>2);
4. KeyOut[2] = ((KeyIn[1]&0x03)<<5) | (KeyIn[2]>>3);
5. KeyOut[3] = ((KeyIn[2]&0x07)<<4) | (KeyIn[3]>>4);
6. KeyOut[4] = ((KeyIn[3]&0x0F)<<3) | (KeyIn[4]>>5);
7. KeyOut[5] = ((KeyIn[4]&0x1F)<<2) | (KeyIn[5]>>6);
8. KeyOut[6] = ((KeyIn[5]&0x3F)<<1) | (KeyIn[6]>>7);
9. KeyOut[7] = KeyIn[6] & 0x7F;
10. ((DWORD\*)KeyOut)[0] <<= 1;
11. ((DWORD\*)KeyOut)[1] <<= 1;
12. ((DWORD\*)KeyOut)[0] &= 0xfefefefe;
13. ((DWORD\*)KeyOut)[1] &= 0xfefefefe;
14. Assume bytes(s, e, l) returns bytes from s to e of the byte
15. array l. Assume concat(a1, a2) returns byte array containing
16. the bytes of array a1 followed by the bytes from byte array a2.
17. LMDESECB(Input, Sk, Output)
18. SET k1 to bytes(0, 7, Sk)
19. CALL InitLMKey(k1, k3)
20. SET k2 to bytes(8, 15, Sk)
21. CALL InitLMKey(k2, k4)
22. SET i1 to bytes(0, 7, Input)
23. SET i2 to bytes(8, 15, Input)
24. CALL DES\_ECB(i1, k3, &output1)
25. CALL DES\_ECB(i2, k4, &output2)
26. SET Output to concat(output1, output2)

[<107> Section 3.4.5.3.2](#Appendix_A_Target_107): Except in Windows NT 3.1, Windows encrypts using the negotiated encryption algorithm and the session key. Windows NT 3.1 encryption is described in the preceding product behavior note.

[<108> Section 3.4.5.3.2](#Appendix_A_Target_108): Except in Windows NT 3.1, Windows encrypts using the negotiated encryption algorithm and the session key. Windows NT 3.1 encryption is described in a preceding product behavior note in this section.

[<109> Section 3.4.5.3.2](#Appendix_A_Target_109): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<110> Section 3.4.5.3.4](#Appendix_A_Target_110): Except in Windows NT 3.1, Windows encrypts by using the negotiated encryption algorithm and the jsession key. For Windows NT 3.1, encrypt as described in the product behavior note in section [3.4.5.3.2](#Section_3d11001b56594eeaa8dfacdd8f478490).

[<111> Section 3.4.5.3.4](#Appendix_A_Target_111): Except in Windows NT 3.1, Windows encrypts by using the negotiated encryption algorithm and the session key. For Windows NT 3.1, encrypt as described in the product behavior note in section 3.4.5.3.2.

[<112> Section 3.4.5.3.4](#Appendix_A_Target_112): Except in Windows NT 3.1, Windows encrypts using the negotiated encryption algorithm and the session key. For Windows NT 3.1, encrypt as described in the product behavior note in section 3.4.5.3.2.

[<113> Section 3.4.5.3.4](#Appendix_A_Target_113): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<114> Section 3.4.5.3.5](#Appendix_A_Target_114): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<115> Section 3.4.5.4.1](#Appendix_A_Target_115): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<116> Section 3.4.5.4.2](#Appendix_A_Target_116): Windows clients call the NetrDatabaseSync2 method in a loop until all database records are received.

[<117> Section 3.4.5.4.2](#Appendix_A_Target_117): On receiving the STATUS\_MORE\_ENTRIES status code, Windows clients continue calling the NetrDatabaseSync2 routine in a loop until all missing database entries are received. The client terminates the loop on a computer shutdown notification.

[<118> Section 3.4.5.4.2](#Appendix_A_Target_118): Windows clients re-establish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<119> Section 3.4.5.4.4](#Appendix_A_Target_119): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<120> Section 3.4.5.5.4](#Appendix_A_Target_120): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<121> Section 3.4.5.5.6](#Appendix_A_Target_121): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<122> Section 3.4.5.6.4](#Appendix_A_Target_122): Windows clients reestablish the secure channel with the domain controller upon receiving STATUS\_ACCESS\_DENIED.

[<123> Section 3.4.6.1](#Appendix_A_Target_123): Windows uses 4096. Other implementations can use any value.

[<124> Section 3.4.7](#Appendix_A_Target_124): The new Windows registry settings for the **RequireStrongKey** and **RequireSignOrSeal** variables are loaded from the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and the **RequireStrongKey** and **RequireSignOrSeal** keys.

[<125> Section 3.5.1](#Appendix_A_Target_125): In Windows, the default **DynamicSiteNameTimeout** value is 5 minutes, and the allowed range is 0 minutes to 49 days.

[<126> Section 3.5.1](#Appendix_A_Target_126): **RejectMD5Clients** is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<127> Section 3.5.1](#Appendix_A_Target_127): The **NT4Emulator** ADM element is not implemented in Windows NT.

[<128> Section 3.5.1](#Appendix_A_Target_128): **DCRPCPort** is not supported in Windows NT Server and Windows 2000 Server.

[<129> Section 3.5.3](#Appendix_A_Target_129): The named pipe LSASS is also known by the [**alias**](#gt_d046b6e2-3f79-47e1-87d7-754566744dcd) NETLOGON. The client can use this alias to establish an RPC over named pipes connection. The Netlogon security package functionality is not implemented in Windows NT.

[<130> Section 3.5.3](#Appendix_A_Target_130): Implementations that use the Windows registry to persistently store and retrieve the **RejectMD5Clients** variable use the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and RejectMD5Clients key.

[<131> Section 3.5.3](#Appendix_A_Target_131): Implementations that use the Windows registry to persistently store and retrieve the **SignSecureChannel** variable set the following values:

* RegistryValueName: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueType: 4
* RegistryValue: SignSecureChannel

Windows registry keys and values ([MS-GPSB] section 2.2.5) are be exposed at a specified registry path via the Windows Remote Registry Protocol [[MS-RRP]](%5bMS-RRP%5d.pdf#Section_0fa3191dbb79490a81bd54c2601b7a78). For each abstract data model (ADM) element that is loaded from the registry, there is one instance that is shared between the Windows Remote Registry Protocol and the protocol(s) that use(s) the ADM element. Any changes made to the **RejectMD5Clients** registry key will not be reflected in the ADM elements until the [**Netlogon**](#gt_70771a5a-04a3-447d-981b-e03098808c32) [**server**](#gt_434b0234-e970-4e8c-bdfa-e16a30d96703) is stopped and restarted.

[<132> Section 3.5.3](#Appendix_A_Target_132): Windows NT 4.0 initializes the **StrongKeySupport** value to FALSE.

[<133> Section 3.5.3](#Appendix_A_Target_133): In Windows, **AllowSingleLabelDNSDomain** is configured using the following Windows registry path:

* Registry path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueName: AllowSingleLabelDNSDomain
* RegistryType: DWORD
* Acceptable values: 0 = Disabled, 1 = Enabled
* Default value if not explicitly configured: 0.

[<134> Section 3.5.3](#Appendix_A_Target_134): Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 consider **AllowDnsSuffixSearch** to be FALSE.

[<135> Section 3.5.3](#Appendix_A_Target_135): Windows uses the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters registry path and **SiteName** value.

[<136> Section 3.5.3](#Appendix_A_Target_136): In Windows, **FailedDiscoveryCachePeriod** can be configured using the following Windows registry path:

* Registry path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters
* RegistryValueName: NegativeCachePeriod
* RegistryType: DWORD
* AllowedRange: 0 - 604800 (7 days)
* Default value if not explicitly configured: 45 seconds

[<137> Section 3.5.3](#Appendix_A_Target_137): In Windows, the **CacheEntryValidityPeriod** value is 12 hours, unless changed by an administrator.

[<138> Section 3.5.3](#Appendix_A_Target_138): In Windows, the **CacheEntryPingValidityPeriod** value is 30 minutes, unless changed by an administrator.

[<139> Section 3.5.3](#Appendix_A_Target_139): The Windows registry settings to persistently store and retrieve the **DCRPCPort** variable are the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and **DCRPCPort** key.

[<140> Section 3.5.3](#Appendix_A_Target_140): The Windows registry settings to persistently store and retrieve the **RejectDES** variable are the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and **AllowNT4Crypto** key set to negation of the **RejectDES** variable.

[<141> Section 3.5.3](#Appendix_A_Target_141): In Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista, **RejectDES** is FALSE.

[<142> Section 3.5.3](#Appendix_A_Target_142): The Windows registry settings to persistently store and retrieve the **SiteCoverage** variable are the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and **SiteCoverage** key.

[<143> Section 3.5.4](#Appendix_A_Target_143): Gaps in the [**opnum**](#gt_e127848e-c66d-427d-b3aa-9f904fa4ada7) numbering sequence apply to Windows as follows.

| Opnum | Description |
| --- | --- |
| 47 | Windows uses this method only locally, never remotely. |

[<144> Section 3.5.4.3.1](#Appendix_A_Target_144): The **DsrGetDcNameEx2** method is not supported in Windows NT.

[<145> Section 3.5.4.3.1](#Appendix_A_Target_145): The F bit is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<146> Section 3.5.4.3.1](#Appendix_A_Target_146): The P bit is not implemented in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

[<147> Section 3.5.4.3.1](#Appendix_A_Target_147): Windows implements both the LDAP Ping ([MS-ADTS] section 6.3.3) and the Mailslot Ping ([MS-ADTS] section 6.3.5) methods and uses them to locate a DC ([MS-ADTS] section 6.3.6).

[<148> Section 3.5.4.3.1](#Appendix_A_Target_148): Windows NT does not support [**directory service**](#gt_c36db657-3138-4d9a-9289-ded5cbb8b40e) functions.

[<149> Section 3.5.4.3.1](#Appendix_A_Target_149): In all applicable Windows Server releases except Windows NT, DCs support directory service functions.

[<150> Section 3.5.4.3.1](#Appendix_A_Target_150): In all applicable Windows Server releases except Windows NT, a DC is writable when it hosts a writable copy of the directory service. These DCs are writable unless they are RODCs. A Windows NT DC is writable only if it is a PDC.

[<151> Section 3.5.4.3.1](#Appendix_A_Target_151): The T bit is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<152> Section 3.5.4.3.1](#Appendix_A_Target_152): If neither the R nor S flag is specified, Windows returns the type of name that matches the type of the *DomainName* parameter.

[<153> Section 3.5.4.3.1](#Appendix_A_Target_153): In Windows, if neither the R nor S flags are set in the *Flags* parameter, the behavior is as follows:

* If only one of the **DnsHostName** or **NetbiosComputerName** fields is set in the message, the **DomainControllerName** field is set to that value.
* Otherwise, if both the **DnsHostName** and **NetbiosComputerName** fields are set in the message:
  + If the *DomainName* parameter is equal to the **DnsDomainName** message field, the **DomainControllerName** field is set to the value of the **DnsHostName** message field.
  + If the *DomainName* parameter is equal to the **NetbiosDomainName** message field, the **DomainControllerName** field is set to the value of the **NetbiosComputerName** message field.
  + If the *DomainName* parameter is NULL:
    - If the DC responded to the LDAP message, the **DomainControllerName** field is set to the value of the **DnsHostName** message field.
    - If the DC responded to the mailslot message, the **DomainControllerName** field is set to the value of the **NetbiosComputerName** message field.

[<154> Section 3.5.4.3.1](#Appendix_A_Target_154): In Windows, if neither the R nor S flags are set in the *Flags* parameter, the behavior is as follows:

* If only one of the **DnsDomainName** or **NetbiosDomainName** fields is set in the message, the **DomainName** field is set to that value.
* Otherwise, if both the **DnsDomainName** and **NetbiosDomainName** fields are set in the message:
  + If the *DomainName* parameter of the **DsrGetDcNameEx2** call is equal to the **DnsDomainName** message field, the **DomainName** field is set to the value of the **DnsDomainName** message field.
  + If the *DomainName* parameter of the **DsrGetDcNameEx2** call is equal to the **NetbiosDomainName** message field, the **DomainName** field is set to the value of the **NetbiosDomainName** message field.
  + If the *DomainName* parameter of the **DsrGetDcNameEx2** call is NULL:
    - If the DC responded to the LDAP message, the **DomainName** field is set to the value of the **DnsDomainName** message field.
    - If the DC responded to the mailslot message, the **DomainName** field is set to the value of the **NetbiosDomainName** message field.

[<155> Section 3.5.4.3.2](#Appendix_A_Target_155): DsrGetDcNameEx is not supported in Windows NT.

[<156> Section 3.5.4.3.3](#Appendix_A_Target_156): DsrGetDcName is not supported in Windows NT.

[<157> Section 3.5.4.3.4](#Appendix_A_Target_157): NetrGetDCName is supported in Windows NT Server 3.1. It is superseded by the [DsrGetDcNameEx2](#Section_fb8e1146a0454c3198d1c68507ad5620) method (section 3.5.4.3.1) in Windows 2000.

[<158> Section 3.5.4.3.4](#Appendix_A_Target_158): Windows implements both the LDAP ping-based method ([MS-ADTS] section 6.3.3) and the mailslot message-based method ([MS-ADTS] section 6.3.5), and uses those two methods to locate a DC ([MS-ADTS] section 6.3.6).

[<159> Section 3.5.4.3.5](#Appendix_A_Target_159): NetrGetAnyDCName is supported in Windows NT Server 3.1 through Windows NT 4.0. It is superseded by the DsrGetDcNameEx2 method (section 3.5.4.3.1) in Windows 2000.

[<160> Section 3.5.4.3.5](#Appendix_A_Target_160): Windows implements both the LDAP ping-based method ([MS-ADTS] section 6.3.3) and the mailslot ping method ([MS-ADTS] section 6.3.5), and uses those two methods to locate a DC ([MS-ADTS] section 6.3.6).

[<161> Section 3.5.4.3.6](#Appendix_A_Target_161): DsrGetSiteName is not supported in Windows NT.

[<162> Section 3.5.4.3.6](#Appendix_A_Target_162): Windows implements both the LDAP Ping method ([MS-ADTS] section 6.3.3) and the Mailslot Ping method ([MS-ADTS] section 6.3.5), and uses those two methods to locate a DC ([MS-ADTS] section 6.3.6).

[<163> Section 3.5.4.3.7](#Appendix_A_Target_163): [DsrGetDcSiteCoverageW](#Section_6d26f254b1254f0f84411ca66cc93b2f) is not supported in Windows NT.

[<164> Section 3.5.4.3.8](#Appendix_A_Target_164): DsrAddressToSiteNamesW is not supported in Windows NT.

[<165> Section 3.5.4.3.9](#Appendix_A_Target_165): [DsrAddressToSiteNamesExW](#Section_95c432063a184af3928d02d2e0c3d6c1) is not supported in Windows NT.

[<166> Section 3.5.4.3.10](#Appendix_A_Target_166): DsrDeregisterDnsHostRecords is not supported in Windows NT.

[<167> Section 3.5.4.3.11](#Appendix_A_Target_167): DsrUpdateReadOnlyServerDnsRecords is not implemented in Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista.

[<168> Section 3.5.4.3.11](#Appendix_A_Target_168): The normal (writable) DC cannot be a Windows 2000 Server or a Windows Server 2003 DC.

[<169> Section 3.5.4.4.1](#Appendix_A_Target_169): NetrServerReqChallenge is not implemented in Windows NT 3.1.

[<170> Section 3.5.4.4.2](#Appendix_A_Target_170): NetrServerAuthenticate3 is not supported in Windows NT.

[<171> Section 3.5.4.4.2](#Appendix_A_Target_171): In Windows, all machine account names are the name of the machine with a "$" (dollar sign) appended.

[<172> Section 3.5.4.4.2](#Appendix_A_Target_172): Except in Windows NT 4.0, if the value is 5 (UasServerSecureChannel), the server always returns an access-denied error because this functionality is no longer supported. Windows NT 4.0 has configuration parameter options allowing UAS compatibility mode, and if this mode is enabled, the error is not returned and further processing occurs. Otherwise, it returns an access-denied error.

[<173> Section 3.5.4.4.3](#Appendix_A_Target_173): NetrServerAuthenticate2 is used in Windows NT 3.5 and Windows NT 4.0. It is superseded by the NetrServerAuthenticate3 method (section 3.5.4.4.2).

[<174> Section 3.5.4.4.4](#Appendix_A_Target_174): NetrServerAuthenticate is used only in Windows NT Server 3.1. In Windows NT Server 3.5 operating system, it is superseded by the NetrServerAuthenticate2 method (section 3.5.4.4.3).

[<175> Section 3.5.4.4.5](#Appendix_A_Target_175): NetrServerPasswordSet2 is not supported in Windows NT.

[<176> Section 3.5.4.4.5](#Appendix_A_Target_176): By default, the period is 30 days in Windows.

[<177> Section 3.5.4.4.5](#Appendix_A_Target_177): In Windows, all machine account names are the name of the machine with a "$" (dollar sign) appended.

[<178> Section 3.5.4.4.6](#Appendix_A_Target_178): NetrServerPasswordSet is not implemented in Windows NT 3.1.

[<179> Section 3.5.4.4.6](#Appendix_A_Target_179): In Windows, all machine account names are the name of the machine with a "$" (dollar sign) appended.

[<180> Section 3.5.4.4.7](#Appendix_A_Target_180): NetrServerPasswordGet is not supported in Windows NT.

[<181> Section 3.5.4.4.7](#Appendix_A_Target_181): In Windows, all machine account names are the name of the machine with a "$" (dollar sign) appended.

[<182> Section 3.5.4.4.8](#Appendix_A_Target_182): [NetrServerTrustPasswordsGet](#Section_84b0d22a9b2c44328ae04a72eda28ea4) is not supported in Windows NT and Windows 2000 prior to Windows 2000 Server operating system Service Pack 4 (SP4).

[<183> Section 3.5.4.4.8](#Appendix_A_Target_183): In Windows, all machine account names are the name of the machine with a "$" (dollar sign) appended.

[<184> Section 3.5.4.4.9](#Appendix_A_Target_184): NetrLogonGetDomainInfo is not supported in Windows NT.

[<185> Section 3.5.4.4.9](#Appendix_A_Target_185): Verifying that the *WkstaBuffer* parameter is not NULL is not supported in Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008.

[<186> Section 3.5.4.4.9](#Appendix_A_Target_186): Windows uses 4096. Other implementations can use any value.

[<187> Section 3.5.4.4.9](#Appendix_A_Target_187): In Windows, NETLOGON\_ONE\_DOMAIN\_INFO.TrustExtension MaximumLength and Length are set to the size 0x10, and Buffer points to a buffer containing the following fields of a DS\_DOMAIN\_TRUSTSW structure: Flags, ParentIndex, TrustType, TrustAttributes.

[<188> Section 3.5.4.4.9](#Appendix_A_Target_188): If the *wProductType* is VER\_NT\_WORKSTATION, then the string is "Windows Workstation", otherwise the string is "Windows Server".

[<189> Section 3.5.4.4.9](#Appendix_A_Target_189): If both WkstaBuffer.*WorkstationInfo*.*OsVersion* and WkstaBuffer.*WorkstationInfo*.*OsName* are unspecified, Windows 2000, Windows XP, and Windows Server 2003 use the generic string "Windows 2000" to update the **operatingSystem** attribute. If only WkstaBuffer.*WorkstationInfo*.*OsName* is unspecified, Windows 2000, Windows XP, and Windows Server 2003 use the generic string "Windows 2000 Professional" when WkstaBuffer.*WorkstationInfo*.*OsVersion*.*wProductType* is VER\_NT\_WORKSTATION, and otherwise use the string "Windows 2000 Server" to update the **operatingSystem** attribute.

[<190> Section 3.5.4.4.10](#Appendix_A_Target_190): NetrLogonGetCapabilities is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

In Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008, RPC opnum 21 is associated with the following RPC method, which does not perform any protocol-relevant function:

1. NTSTATUS NetrLogonDummyRoutine1(
2. [in, string] LOGONSRV\_HANDLE ServerName,
3. [in, string, unique] wchar\_t\* ComputerName,
4. [in] PNETLOGON\_AUTHENTICATOR Authenticator,
5. [in, out] PNETLOGON\_AUTHENTICATOR ReturnAuthenticator,
6. [in] DWORD QueryLevel,
7. [out, switch\_is(QueryLevel)] PNETLOGON\_DUMMY1 Buffer
8. );

The return type and parameters for NetrLogonDummyRoutine1 take on the same data representation as those for NetrLogonGetCapabilities.

[<191> Section 3.5.4.4.10](#Appendix_A_Target_191): The *ServerCapabilities* parameter is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008. These operating systems supported a dummy buffer type:

[out, switch\_is(QueryLevel)] PNETLOGON\_DUMMY1 Buffer

**Buffer**: A pointer to a byte buffer.

[<192> Section 3.5.4.4.10](#Appendix_A_Target_192): Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 do no processing for this call, and always return 0xC0000002 (STATUS\_NOT\_IMPLEMENTED).

[<193> Section 3.5.4.4.11](#Appendix_A_Target_193): NetrChainSetClientAttributes is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Vista. The normal (writable) DC cannot be a Windows 2000 Server or a Windows Server 2003 DC.

[<194> Section 3.5.4.4.11](#Appendix_A_Target_194): STATUS\_ACCESS\_DENIED is returned if the read-only domain controller, *ChainedFromServerName*, does not have permission to replicate the secrets for the client's computer account identified by *ChainedForClientName*.

[<195> Section 3.5.4.5.1](#Appendix_A_Target_195): NetrLogonSamLogonEx is not supported in Windows NT.

[<196> Section 3.5.4.5.1](#Appendix_A_Target_196): Windows uses the value 0x01 as the representation of TRUE and 0x00 for FALSE.

[<197> Section 3.5.4.5.1](#Appendix_A_Target_197): Bits C and D are not implemented in Windows NT, Windows 2000, and Windows Server 2003.

[<198> Section 3.5.4.5.1](#Appendix_A_Target_198): Except in Windows NT 3.1, Windows decrypts by using the negotiated [**decryption**](#gt_8bf79983-1325-42db-8e2c-520c8ab2ae74) algorithm and the session key. For Windows NT 3.1, decrypt as follows.

1. InitLMKey(KeyIn, KeyOut)
2. KeyOut[0] = KeyIn[0] >> 0x01;
3. KeyOut[1] = ((KeyIn[0]&0x01)<<6) | (KeyIn[1]>>2);
4. KeyOut[2] = ((KeyIn[1]&0x03)<<5) | (KeyIn[2]>>3);
5. KeyOut[3] = ((KeyIn[2]&0x07)<<4) | (KeyIn[3]>>4);
6. KeyOut[4] = ((KeyIn[3]&0x0F)<<3) | (KeyIn[4]>>5);
7. KeyOut[5] = ((KeyIn[4]&0x1F)<<2) | (KeyIn[5]>>6);
8. KeyOut[6] = ((KeyIn[5]&0x3F)<<1) | (KeyIn[6]>>7);
9. KeyOut[7] = KeyIn[6] & 0x7F;
10. ((DWORD\*)KeyOut)[0] <<= 1;
11. ((DWORD\*)KeyOut)[1] <<= 1;
12. ((DWORD\*)KeyOut)[0] &= 0xfefefefe;
13. ((DWORD\*)KeyOut)[1] &= 0xfefefefe;
14. Assume bytes(s, e, l) returns bytes from s to e of the byte
15. array l. Assume concat(a1, a2) returns byte array containing
16. the bytes of array a1 followed by the bytes from byte array a2.
17. LMDESECB(Input, Sk, Output)
18. SET k1 to bytes(0, 7, Sk)
19. CALL InitLMKey(k1, k3)
20. SET k2 to bytes(8, 15, Sk)
21. CALL InitLMKey(k2, k4)
22. SET i1 to bytes(0, 7, Input)
23. SET i2 to bytes(8, 15, Input)
24. CALL DES\_ECB(i1, k3, &output1)
25. CALL DES\_ECB(i2, k4, &output2)
26. SET Output to concat(output1, output2)

[<199> Section 3.5.4.5.1](#Appendix_A_Target_199): Except in Windows NT 3.1, Windows decrypts by using the negotiated decryption algorithm and the session key. For Windows NT 3.1, decrypt as described in the product behavior note earlier in the section.

[<200> Section 3.5.4.5.1](#Appendix_A_Target_200): Except in Windows NT 3.1, Windows decrypts by using the negotiated decryption algorithm and the session key. For Windows NT 3.1, decrypt as described in the product behavior note earlier in the section.

[<201> Section 3.5.4.5.1](#Appendix_A_Target_201): Except in Windows NT and Windows 2000, Windows supports verifying whether a correct combination of *LogonLevel* and *ValidationLevel* is supplied. The data is opaque to Netlogon and is passed unexamined to the package specified by the **PackageName** field of the [NETLOGON\_GENERIC\_INFO](#Section_fe2775d4a3e24971a2558eef8dd27a27) structure. For more information, see section 3.2.4.1.

[<202> Section 3.5.4.5.1](#Appendix_A_Target_202): Windows NT and Windows 2000 do not verify whether a correct combination of *LogonLevel* and *ValidationLevel* is supplied.

[<203> Section 3.5.4.5.2](#Appendix_A_Target_203): [NetrLogonSamLogonWithFlags](#Section_d17f1077de4b4fcd886739068cb789f5) is not supported in Windows NT and Windows 2000 prior to Windows 2000 Server SP4.

[<204> Section 3.5.4.5.2](#Appendix_A_Target_204): Windows uses the value of 0x01 as the representation of TRUE and 0x00 for FALSE.

[<205> Section 3.5.4.5.2](#Appendix_A_Target_205): Bits C and D are not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.

[<206> Section 3.5.4.5.3](#Appendix_A_Target_206): NetrLogonSamLogon is only used in Windows NT 4.0. It is superseded by the NetrLogonSamLogonWithFlags method (section 3.5.4.5.2).

[<207> Section 3.5.4.5.4](#Appendix_A_Target_207): NetrLogonSamLogoff is not available in Windows NT 3.1.

[<208> Section 3.5.4.5.4](#Appendix_A_Target_208): Windows NT servers support logoff updates.

[<209> Section 3.5.4.6.1](#Appendix_A_Target_209): NetrDatabaseDeltas is not available in Windows NT 3.1.

[<210> Section 3.5.4.6.1](#Appendix_A_Target_210): All applicable Windows Server releases stop including elements in the returned *DeltaArray* after the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter.

[<211> Section 3.5.4.6.1](#Appendix_A_Target_211): Windows limits the number of records to approximately 1,000 records per call.

[<212> Section 3.5.4.6.1](#Appendix_A_Target_212): The server maintains and updates a state that indicates the client progress in the synchronization protocol, as described in section [3.6](#Section_f28f9dc8eeb241129eeca466f639c761).

[<213> Section 3.5.4.6.2](#Appendix_A_Target_213): NetrDatabaseSync2 is not available in Windows NT 3.1, Windows NT Server 3.1, Windows NT 3.5, Windows 7, or Windows Server 2008 R2.

[<214> Section 3.5.4.6.2](#Appendix_A_Target_214): Windows stops including elements in the returned *DeltaArray* once the size of the returned data equals or exceeds the value of the *PreferredMaximumLength* parameter.

[<215> Section 3.5.4.6.2](#Appendix_A_Target_215): Windows limits the number of records to approximately 1,000 records per call.

[<216> Section 3.5.4.6.3](#Appendix_A_Target_216): The NetrDatabaseSync method was used in Windows NT prior to Windows NT 4.0. It is superseded by the [NetrDatabaseSync2](#Section_31fc80bd4f4d4512a792e488bb78f6a0) method.

[<217> Section 3.5.4.6.4](#Appendix_A_Target_217): NetrDatabaseRedo is not available in Windows NT 3.1, Windows NT Server 3.1, Windows NT 3.5, Windows 7, or Windows Server 2008 R2.

[<218> Section 3.5.4.7.1](#Appendix_A_Target_218): [DsrEnumerateDomainTrusts](#Section_f98236242b34415cbdca9f9a6d97016b) is not supported in Windows NT.

[<219> Section 3.5.4.7.2](#Appendix_A_Target_219): NetrEnumerateTrustedDomainsEx is not supported in Windows NT.

[<220> Section 3.5.4.7.3](#Appendix_A_Target_220): NetrEnumerateTrustedDomains is not available in Windows NT prior to Windows NT 4.0.

[<221> Section 3.5.4.7.4](#Appendix_A_Target_221): NetrGetForestTrustInformation is not supported in Windows NT and Windows 2000 Server prior to Windows 2000 Server SP4.

[<222> Section 3.5.4.7.5](#Appendix_A_Target_222): DsrGetForestTrustInformation is not supported in Windows NT and Windows 2000 prior to Windows 2000 Server SP4.

[<223> Section 3.5.4.7.6](#Appendix_A_Target_223): NetrServerGetTrustInfo is not supported in Windows NT and Windows 2000 prior to Windows 2000 Server SP4.

[<224> Section 3.5.4.8.1](#Appendix_A_Target_224): NetrLogonGetTrustRid is not supported in Windows NT.

[<225> Section 3.5.4.8.1](#Appendix_A_Target_225): Windows NT, Windows 2000, Windows XP, and Windows Server 2003 allow the call to succeed. Other Windows releases return ERROR\_ACCESS\_DENIED if not local.

[<226> Section 3.5.4.8.2](#Appendix_A_Target_226): NetrLogonComputeServerDigest is not implemented in Windows NT.

[<227> Section 3.5.4.8.2](#Appendix_A_Target_227): When the previous password is not present, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server operating system use an uninitialized value to compute the *OldMessageDigest* parameter.

[<228> Section 3.5.4.8.3](#Appendix_A_Target_228): NetrLogonComputeClientDigest is not implemented in Windows NT.

[<229> Section 3.5.4.8.4](#Appendix_A_Target_229): NetrLogonSendToSam is not supported in Windows NT.

[<230> Section 3.5.4.8.5](#Appendix_A_Target_230): NetrLogonSetServiceBits is not supported in Windows NT.

[<231> Section 3.5.4.8.5](#Appendix_A_Target_231): The C flag is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<232> Section 3.5.4.8.5](#Appendix_A_Target_232): The C flag is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.

[<233> Section 3.5.4.8.5](#Appendix_A_Target_233): Windows NT, Windows 2000, Windows XP, and Windows Server 2003 allow the call to succeed. Other Windows releases return ERROR\_ACCESS\_DENIED if not local.

[<234> Section 3.5.4.8.6](#Appendix_A_Target_234): NetrLogonGetTimeServiceParentDomain is not supported in Windows NT.

[<235> Section 3.5.4.8.6](#Appendix_A_Target_235): The Netlogon client ignores this value if *ServerName* is not a domain controller.

[<236> Section 3.5.4.8.6](#Appendix_A_Target_236): Windows NT, Windows 2000, Windows XP, and Windows Server 2003 allow the call to succeed.

[<237> Section 3.5.4.9.1](#Appendix_A_Target_237): NetrLogonControl2Ex executes Windows-specific admininstrative actions and is not available in Windows NT prior to Windows NT 4.0.

[<238> Section 3.5.4.9.1](#Appendix_A_Target_238): The following restrictions apply to the values of the *FunctionCode* parameter. The error ERROR\_NOT\_SUPPORTED is returned if one of these values is used.

The following values are not supported on Windows NT 4.0:

* NETLOGON\_CONTROL\_CHANGE\_PASSWORD (0x00000009)
* NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A)
* NETLOGON\_CONTROL\_FORCE\_DNS\_REG (0x0000000B)
* NETLOGON\_CONTROL\_QUERY\_DNS\_REG (0x0000000C)
* NETLOGON\_CONTROL\_BACKUP\_CHANGE\_LOG (0x0000FFFC)
* NETLOGON\_CONTROL\_TRUNCATE\_LOG (0x0000FFFD)
* NETLOGON\_CONTROL\_SET\_DBFLAG (0x0000FFFE)
* NETLOGON\_CONTROL\_BREAKPOINT (0x0000FFFF)

The following values are not supported on Windows 2000 Server:

* NETLOGON\_CONTROL\_TC\_VERIFY (0x0000000A)
* NETLOGON\_CONTROL\_FORCE\_DNS\_REG (0x0000000B)
* NETLOGON\_CONTROL\_QUERY\_DNS\_REG (0x0000000C)

The following values are not supported on Windows 7 and Windows Server 2008 R2:

* NETLOGON\_CONTROL\_REPLICATE (0x00000002)
* NETLOGON\_CONTROL\_SYNCHRONIZE (0x00000003)
* NETLOGON\_CONTROL\_PDC\_REPLICATE (0x00000004)
* NETLOGON\_CONTROL\_BACKUP\_CHANGE\_LOG (0x0000FFFC)

No restrictions apply in Windows Server 2003, Windows Vista, and Windows Server 2008.

[<239> Section 3.5.4.9.1](#Appendix_A_Target_239): NETLOGON\_CONTROL\_REPLICATE is supported on servers that are Windows NT 4.0 BDCs; otherwise, the ERROR\_NOT\_SUPPORTED error is returned from a server that is not a Windows NT 4.0 BDC.

[<240> Section 3.5.4.9.1](#Appendix_A_Target_240): NETLOGON\_CONTROL\_SYNCHRONIZE is supported on Windows NT 4.0 BDCs; otherwise, the ERROR\_NOT\_SUPPORTED error is returned from a server that is not a Windows NT 4.0 BDC.

[<241> Section 3.5.4.9.1](#Appendix_A_Target_241): On a Windows NT, Windows 2000, or Windows XP DC, ERROR\_NOT\_SUPPORTED is returned. The server implementation decides how the [**DNS**](#gt_604dcfcd-72f5-46e5-85c1-f3ce69956700) update status is recorded.

[<242> Section 3.5.4.9.1](#Appendix_A_Target_242): In Windows, the server copies to a backup file the contents of a file that contains a cache of database changes.

[<243> Section 3.5.4.9.1](#Appendix_A_Target_243): In Windows, the server truncates the contents of a debug file that contains debugging information about the Netlogon service operations.

[<244> Section 3.5.4.9.1](#Appendix_A_Target_244): In Windows, the server sets the level of verbosity of output into the debug file that contains debugging information about the Netlogon service operations. The level of verbosity to set is specified in the **DebugFlag** field of the *Data* parameter.

[<245> Section 3.5.4.9.1](#Appendix_A_Target_245): In Windows, if the [NetrLogonControl2Ex](#Section_df7e5dd1ebcc47549da02e0bded82d29) method is called with the function code NETLOGON\_CONTROL\_BREAKPOINT and the operating system is not a [**checked build**](#gt_cd33ef8c-8d58-43b6-9273-fa308fc1caf1), the method returns ERROR\_NOT\_SUPPORTED.

[<246> Section 3.5.4.9.1](#Appendix_A_Target_246): In Windows, the server breaks into the debugger if it is attached to the computer that supports debugging.

[<247> Section 3.5.4.9.1](#Appendix_A_Target_247): The NETLOGON\_INFO\_4 structure is not supported in Windows NT.

[<248> Section 3.5.4.9.1](#Appendix_A_Target_248): Windows NT 4.0 BDCs force an immediate partial synchronization of all databases.

[<249> Section 3.5.4.9.1](#Appendix_A_Target_249): Windows NT 4.0 BDCs force an immediate full synchronization of all databases.

[<250> Section 3.5.4.9.1](#Appendix_A_Target_250): Windows NT 4.0 PDCs immediately send announcement messages to request each BDC to replicate the database.

[<251> Section 3.5.4.9.1](#Appendix_A_Target_251): Windows NT and Windows 2000 DCs return ERROR\_NOT\_SUPPORTED.

[<252> Section 3.5.4.9.1](#Appendix_A_Target_252): Windows NT and Windows 2000 DCs return ERROR\_NOT\_SUPPORTED.

[<253> Section 3.5.4.9.2](#Appendix_A_Target_253): NetrLogonControl2 is not supported in Windows NT 3.1.

[<254> Section 3.5.4.9.3](#Appendix_A_Target_254): NetrLogonControl is not available in Windows NT 3.1.

[<255> Section 3.5.4.9.3](#Appendix_A_Target_255): The *FunctionCode* parameter is restricted to the following values. If any other value is used, the error code ERROR\_NOT\_SUPPORTED is returned.

Windows NT 4.0:

* NETLOGON\_CONTROL\_QUERY (0x00000001)
* NETLOGON\_CONTROL\_REPLICATE (0x00000002)
* NETLOGON\_CONTROL\_SYNCHRONIZE (0x00000003)
* NETLOGON\_CONTROL\_PDC\_REPLICATE (0x00000004)

Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008:

* NETLOGON\_CONTROL\_QUERY (0x00000001)
* NETLOGON\_CONTROL\_REPLICATE (0x00000002)
* NETLOGON\_CONTROL\_SYNCHRONIZE (0x00000003)
* NETLOGON\_CONTROL\_PDC\_REPLICATE (0x00000004)
* NETLOGON\_CONTROL\_BACKUP\_CHANGE\_LOG (0x0000FFFC)
* NETLOGON\_CONTROL\_TRUNCATE\_LOG (0x0000FFFD)
* NETLOGON\_CONTROL\_BREAKPOINT (0x0000FFFF)

For all windows releases except Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008:

* NETLOGON\_CONTROL\_QUERY (0x00000001)
* NETLOGON\_CONTROL\_TRUNCATE\_LOG (0x0000FFFD)
* NETLOGON\_CONTROL\_BREAKPOINT (0x0000FFFF)

[<256> Section 3.5.4.10](#Appendix_A_Target_256): The Netlogon client implementations in Windows ignore these methods. The Netlogon server returns STATUS\_NOT\_IMPLEMENTED.

[<257> Section 3.5.6](#Appendix_A_Target_257): The new **SignSecureChannel** value is loaded into the Windows registry from the HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Netlogon\Parameters registry path and SignSecureChannel key.

[<258> Section 3.6](#Appendix_A_Target_258): Netlogon replication requires the PDC to run Windows NT Server 4.0, Windows 2000 Server, or Windows Server 2003, while BDCs run Windows NT Server 4.0. Windows Server 2008 does not support replication to Windows NT 4.0 BDCs.

[<259> Section 3.6.4.1](#Appendix_A_Target_259): To indicate such a local condition, the PDC returns a value of 0xC0000134 as the return value of the NetrDatabaseDeltas call. For example, the PDC maintains a partial database state cached in memory that the PDC can use for processing partial synchronization requests. If the cached information is not available (for example, if the cache gets flushed), the PDC returns the error code 0xC0000134.

[<260> Section 3.6.5.1](#Appendix_A_Target_260): A separate timer is used on the PDC to time out announcements sent to the BDCs. A BDC is deemed as processing the announcement request until it finishes the processing by completing a synchronization request as described in the following sections. During that time, no additional announcements are sent to the BDC. If a BDC doesn't respond with a synchronization request within the time-out period as set by the timer, the announcement is deemed as timed out.

[<261> Section 3.6.6](#Appendix_A_Target_261): In all of the message processing scenarios described in section [3.6.4](#Section_f310867bca064d37addff7dcd9f97ad7), Netlogon performs a [**full database synchronization**](#gt_40bb6bec-5505-4967-b4ad-371f47cd70c9).

# Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

* A document revision that incorporates changes to interoperability requirements.
* A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact [dochelp@microsoft.com](mailto:dochelp@microsoft.com).

| Section | Description | Revision class |
| --- | --- | --- |
| [7](#Section_0c858a52732a43ec85dde44b357c1898) Appendix B: Product Behavior | Added Windows Server to the list of applicable products and product behavior notes. | Major |

# Index

A

Abstract data model

[client](#section_fd1e918135a045d3b39cb7453dfc0af5) 122

[Netlogon as security support provider](#section_a7bd20030d614686aa6e89336cec83a1) 113

[Netlogon common authentication](#section_708b71329e72447c992bd0bef4078f81) 100

[Netlogon NT replication](#section_2d0fcdfaa5d64c20869d12f6383c7271) 217

[pass-through authentication](#section_1875a45ababe4ab4a4c26abe02ab6858) 112

[server](#section_b8d168acebb642f4bfb27a84377f2cbc) 137

[Account database replication](#section_7afa81d37f3e4dc2990a901d7fec94d3) 22

[Account database replication messages and structures](#section_c4adbfb3678b4996860f3602709558b9) 63

Account database replication methods ([section 3.4.5.4](#section_a66d14b214004a908219c24feb03da49) 132, [section 3.4.5.4.1](#section_d754d58d6b0d479e92f48e70bdbf53e0) 132)

[Account Database Replication Methods method](#section_5657e68eab5b4d9998b80fcaa1bdffc6) 184

[Administrative services](#section_43e743b5821441d19d3bda53eed388db) 23

Administrative services methods ([section 3.4.5.7](#section_b3354c5794f84479af88ed053bb2e30d) 136, [section 3.5.4.9](#section_647e0ebb338f499fabbc8f82adcb36ff) 208)

[Administrative Services Methods method](#section_647e0ebb338f499fabbc8f82adcb36ff) 208

[Administrative services structures](#section_3b7ad20ab8c64191971e8b96f85d0899) 92

[Applicability](#section_c3fecc36896f4e479595910561ed4927) 27

Authentication

pass-through ([section 1.3.1](#section_70697480f28548369ca77bb52f18c6af) 20, [section 1.3.2](#section_08b36439331a4e2089a512f3fab33dfc) 21)

[pass-through - structures](#section_d76f87d0b8a142e8b3b147ab47444cbc) 51

B

[Basic structures](#section_5fc4156477124f478ca634edc1721bae) 29

C

[Calling DsrAddressToSiteNamesExW](#section_6fc609e0a915432389f6eac6148f99e2) 125

[Calling DsrAddressToSiteNamesW](#section_6d3e211a992f4e3e984ac7982ec179af) 125

[Calling DsrDeregisterDnsHostRecords](#section_68a21831717c46d1836f3316042f72db) 125

[Calling DsrEnumerateDomainTrusts](#section_ed0f00a662e04c9c98cc69a7eaf108e0) 134

[Calling DsrGetDcName](#section_76967d78c4bc49dc80c2a95b34ff5193) 124

[Calling DsrGetDcNameEx](#section_b6bab64ad0714ec19a43a04887a5c65f) 124

[Calling DsrGetDcNameEx2](#section_f0e800d0e5d640849a62d761b52dc74e) 124

[Calling DsrGetDcSiteCoverageW](#section_0e598aeb858c4a0f8b0f6681492b058d) 125

[Calling DsrGetForestTrustInformation](#section_51cb0c79f5a546ecbad7d8e5c9fca54a) 134

[Calling DsrGetSiteName](#section_e1ac162c591e41188909a726a6d6454e) 125

[Calling methods not requiring session-key establishment](#section_6b7f7a1c83b7452c9b7b2ece221e236d) 110

[Calling methods requiring session-key establishment](#section_f61c3f4a53ff4f3090066d93a2162ef8) 109

[Calling NetrEnumerateTrustedDomains](#section_27071459df0443858b61d3dc6e89d240) 134

[Calling NetrEnumerateTrustedDomainsEx](#section_d4247996d6164e14b9163c296d307370) 134

[Calling NetrGetAnyDCName](#section_2d1c3201e93e4862844b716bf9aa90ad) 125

[Calling NetrGetDCName](#section_14ccf6453b7f41a2b0895767b6d66ab6) 125

[Calling NetrLogonComputeClientDigest](#section_1bf3702bbe13464aad5e6be0fe210c90) 135

[Calling NetrLogonComputeServerDigest](#section_6ba367041d2a41389361ad6c4d6960dd) 135

[Calling NetrLogonControl](#section_d30fb91376a34458a80bc99422591bce) 136

[Calling NetrLogonControl2](#section_0b09479f549f414d9d9fb5a61559ada1) 136

[Calling NetrLogonControl2Ex](#section_5c506b48dd6b40209a504f93b9f8c7c1) 136

[Calling NetrLogonGetDomainInfo](#section_bae4908f09c64ace89ce0420cbb57a9e) 128

[Calling NetrLogonGetTimeServiceParentDomain](#section_4b5b732d18d0471d83a731159ea21f51) 135

[Calling NetrLogonGetTrustRid](#section_085037e0bf694730813e728c5a4d181a) 135

[Calling NetrLogonSamLogoff](#section_4100eb8d799d44918ffb9f7cf84a07ab) 132

[Calling NetrLogonSamLogon](#section_20cf9342c1fa49ada9a96d5f52e444fd) 131

[Calling NetrLogonSamLogonEx](#section_3d11001b56594eeaa8dfacdd8f478490) 129

[Calling NetrLogonSamLogonWithFlags](#section_5b83bc7bca2b4e0199148b58ca8879c9) 130

[Calling NetrLogonUasLogoff](#section_ea345277fe694b93b82dd3781f3d9cee) 136

[Calling NetrLogonUasLogon](#section_a1432738dc134ee8b669211b0335c9f9) 136

[Calling NetrServerAuthenticate](#section_7a3cf5c24513424fad98b7fa19ad9593) 126

[Calling NetrServerAuthenticate2](#section_53669e2c293e49e6925dc37558a83391) 126

[Calling NetrServerAuthenticate3](#section_5ce4f403c16e42bc9c6e30d7e319feac) 125

[Calling NetrServerGetTrustInfo](#section_6482836222d940d48cc2bfad92f50964) 134

[Calling NetrServerPasswordSet](#section_0be5436ec68c46478ecafe0be3512b9b) 127

[Calling NetrServerPasswordSet2](#section_b348c16e5cdb4414876de8b0e12fbae0) 126

[Calling NetrServerReqChallenge](#section_bde2f7752042409d9ea41d0386d931c3) 125

[Calling NetrServerTrustPasswordsGet](#section_d36ad62ac4f247f7be279efdc3d5f319) 128

[Capability negotiation](#section_b5ad98b323be467e91cda580aab8abaf) 27

[Change tracking](#section_62cbfaee898d465bb44cf380deeb696b) 276

Client

[abstract data model](#section_fd1e918135a045d3b39cb7453dfc0af5) 122

[higher-layer triggered events](#section_41344b38080b4a55afa2e45997273a80) 124

[initialization](#section_8db09e2864ff45a78219943405a74b56) 123

[local events](#section_b6a8355236164e2ebdc94f9c52ca2ba5) 137

[message processing](#section_63e975f1e219416e96c4ee2a30bf73b0) 124

[netlogon interface](#section_2e745bde2f654857bd3c7de7b191c35a) 122

[overview](#section_2e745bde2f654857bd3c7de7b191c35a) 122

[Pass-Through Authentication Methods method](#section_c3eda426dd4f494f8c3a97c0aa479cc9) 129

[sequencing rules](#section_63e975f1e219416e96c4ee2a30bf73b0) 124

[timers](#section_b9ebbb2e8e894db98a9beab526d5e0ca) 123

[Common data types](#section_0c8cf381ddf44dd5b20015c2824e41a9) 29

[Cryptographic values for session key validation example](#section_07ab6badb0d34978825ca1b748967604) 228

[Cryptographic values for session key validation.](#section_07ab6badb0d34978825ca1b748967604) 228

[CYPHER\_BLOCK structure](#section_56a8d298dbeb4eb5ad9876536ec352f8) 29

D

Data model - abstract

[client](#section_fd1e918135a045d3b39cb7453dfc0af5) 122

[Netlogon as security support provider](#section_a7bd20030d614686aa6e89336cec83a1) 113

[Netlogon common authentication](#section_708b71329e72447c992bd0bef4078f81) 100

[Netlogon NT replication](#section_2d0fcdfaa5d64c20869d12f6383c7271) 217

[pass-through authentication](#section_1875a45ababe4ab4a4c26abe02ab6858) 112

[server](#section_b8d168acebb642f4bfb27a84377f2cbc) 137

Data types

[common - overview](#section_0c8cf381ddf44dd5b20015c2824e41a9) 29

[enumerated types](#section_c3a0defffd1b4df9850f420cb8a224f5) 29

[overview](#section_0c8cf381ddf44dd5b20015c2824e41a9) 29

[structures](#section_c3a0defffd1b4df9850f420cb8a224f5) 29

[Databases - account database replication](#section_7afa81d37f3e4dc2990a901d7fec94d3) 22

DC location methods ([section 3.4.5.1](#section_ec4814a5b28e41369f3d3860b3753af7) 124, [section 3.5.4.3](#section_2c26616cfe894d0288aea56356e0f512) 147)

[DC Location Methods method](#section_2c26616cfe894d0288aea56356e0f512) 147

[DC location structure](#section_94c3b27ad8064eacbfe15a48e63eeca9) 31

[Determining client privileges method](#section_1ec948862b6445afb68e3d9faa36617c) 147

[Directory service schema elements](#section_6e72c5303cc14f0d9a71b3df690721ee) 98

[Domain members - Netlogon operational flow](#section_47389962d4734d1c932bf20cdcb47d64) 23

Domain trust methods ([section 3.4.5.5](#section_f01e2c4debf8491b988170c044ed0fed) 134, [section 3.5.4.7](#section_d6ee9b3a1cf24719a82773f2e0298336) 190)

[Domain Trust Methods method](#section_d6ee9b3a1cf24719a82773f2e0298336) 190

[Domain trust structures](#section_26bc3213bff74ed5ac5b651bab12d874) 89

Domain trusts ([section 1.3.2](#section_08b36439331a4e2089a512f3fab33dfc) 21, [section 1.3.5](#section_a7aa8f241cac469b8671ef6c7d31d5e5) 23)

[DOMAIN\_CONTROLLER\_INFOW structure](#section_9b85a7a48d344b9e9500bf8644ebfc06) 31

[DOMAIN\_NAME\_BUFFER structure](#section_11743dc47a2d4464b35150aeb8801b8b) 89

[DS\_DOMAIN\_TRUSTSW structure](#section_7de9866ed3ef4a9f98a5c2dcff1e61c1) 89

[DsrAddressToSiteNamesExW method](#section_95c432063a184af3928d02d2e0c3d6c1) 162

[DsrAddressToSiteNamesW method](#section_0731ce2efde2405cb7d7c9012df9d718) 161

[DsrDeregisterDnsHostRecords method](#section_db6c9aad573640c5af86538dd439134c) 162

[DsrEnumerateDomainTrusts method](#section_f98236242b34415cbdca9f9a6d97016b) 190

[DsrGetDcName method](#section_86a3fa5b1f0e412a942f33a10e5e9eff) 158

[DsrGetDcNameEx method](#section_5de19b7e4ce34cc4978f8959f46797ba) 157

[DsrGetDcNameEx2 method](#section_fb8e1146a0454c3198d1c68507ad5620) 147

[DsrGetDcSiteCoverageW method](#section_6d26f254b1254f0f84411ca66cc93b2f) 160

[DsrGetForestTrustInformation method](#section_8bff4d0be06c4c3a8bd9b0e2a7f2b06b) 195

[DsrGetSiteName method](#section_2b0173e28c454fde8967ad1cbbc7e593) 159

[DsrUpdateReadOnlyServerDnsRecords method](#section_e83df1615c134520ae5a79218ed0bb19) 163

E

[Elements - directory service schema](#section_6e72c5303cc14f0d9a71b3df690721ee) 98

[ENCRYPTED\_LM\_OWF\_PASSWORD](#section_30a12be7a4ed4ef2bd8883961edb8f26) 30

[ENCRYPTED\_NT\_OWF\_PASSWORD](#section_f7458576d53847cdb387b6f98449a0ee) 30

[Enumerated types](#section_c3a0defffd1b4df9850f420cb8a224f5) 29

Events

[local - client](#section_b6a8355236164e2ebdc94f9c52ca2ba5) 137

[local - server](#section_4d79a456cd4e4474ae9c60d2143a0e57) 215

[timer - server](#section_8bcabeb0ac8f48a9a5c9fa5e968eae88) 215

Examples

[cryptographic values for session key validation](#section_07ab6badb0d34978825ca1b748967604) 228

[netrlogonsamlogon with secure channel](#section_3c4678e3a52848fea9ed15b2319f7698) 223

[NetrLogonSamLogon with secure channel example](#section_3c4678e3a52848fea9ed15b2319f7698) 223

[overview](#section_513bcdd9536647a1b9e7b9385c04cae2) 223

F

[Fields - vendor-extensible](#section_75eb779b284b47d78aa1069ad71928a7) 28

[Full IDL](#section_89f9b028ee684fe2afcacc188f7079f7) 232

G

[Generic pass-through](#section_fe2775d4a3e24971a2558eef8dd27a27) 112

[Glossary](#section_b5e7d25a40b241c8961198f53358af66) 10

[GROUP\_MEMBERSHIP structure](#section_efb926f648c34c298a4586a67bfaaf27) 55

H

[Higher-layer triggered events - client](#section_41344b38080b4a55afa2e45997273a80) 124

I

[IDL](#section_89f9b028ee684fe2afcacc188f7079f7) 232

[Implementer - security considerations](#section_0b6a8035850e4b1195cd1717ed2516fe) 230

[Index of security parameters](#section_d1369c2670ce4c768a29f10cccead4a5) 231

[Informative references](#section_e5df11eeeefe4fc295bd489e86f22292) 19

Initialization

[client](#section_8db09e2864ff45a78219943405a74b56) 123

[Netlogon as security support provider](#section_7ce8f1e1a8dc463696f1551805fb8a9f) 114

[Netlogon common authentication](#section_7c6a6ec2e1c943ba9f0cd65534f6c7ad) 102

[Netlogon NT replication](#section_b3773acfb5aa488c93550ad61767e4f2) 218

[Pass-through authentication](#section_2c9e1afa6b4d4101ac5f1fe325c213fe) 112

[server](#section_f8c12682fd984c1a8b0ab6e153f96186) 140

Interfaces - client

[netlogon](#section_2e745bde2f654857bd3c7de7b191c35a) 122

[Introduction](#section_19896c1c7e64419ba759a9dc5662a780) 10

[IPv4\_Sockaddr packet](#section_75981bfba7bb41bc8705388531af6ed8) 34

[IPv6\_Sockaddr packet](#section_f8e21b2b6ea54eb9a350acdabe33cc93) 34

L

[LM\_CHALLENGE structure](#section_bb8eca9041bc4ca48419defdf043e01b) 51

[LM\_OWF\_PASSWORD structure](#section_30a12be7a4ed4ef2bd8883961edb8f26) 30

Local events

[client](#section_b6a8355236164e2ebdc94f9c52ca2ba5) 137

[Netlogon as security support provider](#section_a4eed9f44e4a4f3dab2ee672a4dbdc31) 121

[Netlogon common authentication](#section_6e9975e7c21d4ec5aafc0dfdf7325ebe) 111

[Netlogon NT replication](#section_d5518fac8388477188ead9424229849c) 222

[pass-through authentication](#section_675e0368a23f475196503b29a329bcc8) 113

[server](#section_4d79a456cd4e4474ae9c60d2143a0e57) 215

M

Message processing

[client](#section_63e975f1e219416e96c4ee2a30bf73b0) 124

[Netlogon as security support provider](#section_eaa58b8aae4941bc9c91846d7746535f) 114

[Netlogon common authentication](#section_f4d97830929947c2b0cdb1da9dec520a) 102

Netlogon NT replication ([section 3.6.4](#section_f310867bca064d37addff7dcd9f97ad7) 218, [section 3.6.4.1](#section_724235138903472f865c7b12ade645f4) 218)

[pass-through authentication](#section_785693dfc2484c4596cab17c1a365a9b) 112

[server](#section_256678803d51499bb22819c08eb16b81) 141

Message protection methods ([section 3.4.5.6](#section_609336b586574b6a97e94f41d298cd23) 135, [section 3.5.4.8](#section_fff9e47b029f41e0b48b1f5c5554b68f) 201)

[Message Protection Methods method](#section_fff9e47b029f41e0b48b1f5c5554b68f) 201

[Message protection services](#section_0e2fb98260f84aa98044dbd2160fa268) 23

Messages

[account database replication](#section_c4adbfb3678b4996860f3602709558b9) 63

[common data types](#section_0c8cf381ddf44dd5b20015c2824e41a9) 29

[data types](#section_0c8cf381ddf44dd5b20015c2824e41a9) 29

[overview](#section_cbba90de503448939a10babd9023ee93) 29

[transport](#section_592edbc8f6f140c09ab3fe6725ac6d7e) 29

Methods

[Account Database Replication Methods](#section_5657e68eab5b4d9998b80fcaa1bdffc6) 184

[Administrative Services Methods](#section_647e0ebb338f499fabbc8f82adcb36ff) 208

[DC Location Methods](#section_2c26616cfe894d0288aea56356e0f512) 147

[Determining client privileges](#section_1ec948862b6445afb68e3d9faa36617c) 147

[Domain Trust Methods](#section_d6ee9b3a1cf24719a82773f2e0298336) 190

[Message Protection Methods](#section_fff9e47b029f41e0b48b1f5c5554b68f) 201

[Obsolete Methods](#section_a9dccfcfea6e4f919c0739183708e34e) 214

Pass-Through Authentication Methods ([section 3.4.5.3](#section_c3eda426dd4f494f8c3a97c0aa479cc9) 129, [section 3.5.4.5](#section_24933c92b96540f19e1d74ea27d4813c) 177)

[RPC Binding Handles for Netlogon Methods](#section_3b224201b53143e28c79b61f6dea8640) 146

[Secure Channel Establishment and Maintenance Methods](#section_641f684e080943f38ba92a3754874126) 164

[Methods - Netlogon](#section_a1aa6492171b49cbaf4e991c7461cf56) 24

N

[Negotiated credential computation](#section_594909fd725f45ac979962e4aefe0585) 107

[Netlog negotiable options](#section_5805bc9fe4c94c8ab1913c3a7de7eeed) 104

Netlogon as security support provider

[abstract data model](#section_a7bd20030d614686aa6e89336cec83a1) 113

[initialization](#section_7ce8f1e1a8dc463696f1551805fb8a9f) 114

[local events](#section_a4eed9f44e4a4f3dab2ee672a4dbdc31) 121

[message processing](#section_eaa58b8aae4941bc9c91846d7746535f) 114

[overview](#section_388e4b68f4e44e0498ecdfae7e9b1f01) 113

[sequencing rules](#section_eaa58b8aae4941bc9c91846d7746535f) 114

[timer events](#section_06fe5d6862b445ed9dc7f8188ac6872d) 121

[timers](#section_acdc3f370ba8486fbbc08aa4ff254286) 114

[Netlogon authenticator computation and verification](#section_da7acaa3030b481e979bf58f89389806) 108

Netlogon common authentication

[abstract data model](#section_708b71329e72447c992bd0bef4078f81) 100

[initialization](#section_7c6a6ec2e1c943ba9f0cd65534f6c7ad) 102

[local events](#section_6e9975e7c21d4ec5aafc0dfdf7325ebe) 111

[message processing](#section_f4d97830929947c2b0cdb1da9dec520a) 102

[overview](#section_273b6905782d4a7ea2e44337816916e0) 100

[sequencing rules](#section_f4d97830929947c2b0cdb1da9dec520a) 102

[timer events](#section_0a9c7006b77e4a979660878df7d9966c) 111

[timers](#section_b1bf5a578cf44ceaa792adeec3bc87c4) 102

Netlogon history

[dummy fields in structures](#section_bbc95890215e49a98bb892e723548046) 25

[LAN manager](#section_0c858a52732a43ec85dde44b357c1898) 256

[negotiated flags](#section_7ef41f6d84b346dc92e19f88ae10f9d8) 26

[new methods from existing methods](#section_bcc16d6de9474628a046f5e40cbc6910) 25

[overview](#section_ea995cec27db431a999b99bdc44b92f8) 24

[netlogon interface](#section_2e745bde2f654857bd3c7de7b191c35a) 122

Netlogon NT replication

[abstract data model](#section_2d0fcdfaa5d64c20869d12f6383c7271) 217

[initialization](#section_b3773acfb5aa488c93550ad61767e4f2) 218

[local events](#section_d5518fac8388477188ead9424229849c) 222

message processing ([section 3.6.4](#section_f310867bca064d37addff7dcd9f97ad7) 218, [section 3.6.4.1](#section_724235138903472f865c7b12ade645f4) 218)

[overview](#section_f28f9dc8eeb241129eeca466f639c761) 215

sequencing rules ([section 3.6.4](#section_f310867bca064d37addff7dcd9f97ad7) 218, [section 3.6.4.1](#section_724235138903472f865c7b12ade645f4) 218)

timer events ([section 3.6.5](#section_202c7366b4974c3a914ff8ff35047b90) 220, [section 3.6.5.1](#section_ce890453cb5a4e999a16f56c7c3e9eca) 220)

[timers](#section_6454b09273ec4b02b5d2454655cfed6a) 218

[Netlogon operational flow - domain members](#section_47389962d4734d1c932bf20cdcb47d64) 23

Netlogon Signature Token

[generate initial token](#section_0593a87c7a83423280f8571e34220fed) 116

[overview](#section_2af2dc5f794143aba6d063161a591a6e) 116

[receipt of initial token](#section_4daf7de2197f48eab34cea71773fde9b) 118

[Netlogon structures and methods](#section_a1aa6492171b49cbaf4e991c7461cf56) 24

[NETLOGON\_AUTHENTICATOR structure](#section_76c93227942a4687ab9d9d972ffabdab) 31

[NETLOGON\_CREDENTIAL structure](#section_d55e263271634f6cb6624b870e8cc1cd) 41

[NETLOGON\_DB\_CHANGE\_Announcement\_Message packet](#section_b3a7e5f3d6694f54acb8e85580eaf46d) 63

[NETLOGON\_DELTA\_ACCOUNTS structure](#section_7f60a1a799d849ba91c06e027237b009) 66

[NETLOGON\_DELTA\_ALIAS structure](#section_38155d03b5dc445d9fcba6938be5972d) 68

[NETLOGON\_DELTA\_ALIAS\_MEMBER structure](#section_aeca74675e13417ca4cb71d1f6476090) 69

[NETLOGON\_DELTA\_DELETE\_GROUP structure](#section_3ef0689005194f6e889dec76cd865d7c) 70

[NETLOGON\_DELTA\_DELETE\_USER structure](#section_3fb60f5fe33d427bb540ac3b84342d5d) 70

[NETLOGON\_DELTA\_DOMAIN structure](#section_803be876d7554187a011eaf5bf2755ab) 71

[NETLOGON\_DELTA\_ENUM structure](#section_20e5863c014240f6a914f352a9d66047) 72

[NETLOGON\_DELTA\_ENUM\_ARRAY structure](#section_82d47318c4d8458386a6ce186504bcba) 72

[NETLOGON\_DELTA\_GROUP structure](#section_b7949b4e0fc740d488418d69230e2d79) 73

[NETLOGON\_DELTA\_GROUP\_MEMBER structure](#section_3d4c56361f2a4896a717d8598ffaffab) 78

[NETLOGON\_DELTA\_POLICY structure](#section_b9ee3608efd14d57b4da5a13b9ec1fa1) 79

[NETLOGON\_DELTA\_SECRET structure](#section_ddf4e131ef89425fa70b88fdd73afb51) 81

[NETLOGON\_DELTA\_TRUSTED\_DOMAINS structure](#section_fe95340edb884fdd85c6bc8ad1c4ff8c) 82

[NETLOGON\_DELTA\_TYPE [Protocol]](#section_f8a8cd32426d45f1be45e0dc5c1c1359) 87

[NETLOGON\_DELTA\_TYPE enumeration](#section_f8a8cd32426d45f1be45e0dc5c1c1359) 87

[NETLOGON\_DELTA\_USER structure](#section_c82fcc5a59b647f79f69dec916ebed2c) 77

[NETLOGON\_DOMAIN\_INFO structure](#section_440c3430ed5f481db60274db422df3c8) 46

[NETLOGON\_GENERIC\_INFO structure](#section_c03d6d959b5e43299645eedcdd167f6e) 51

[NETLOGON\_INFO\_1 structure](#section_afeb873c48264beba35cae73a708b108) 93

[NETLOGON\_INFO\_2 structure](#section_c48a87004c174afb8866f0cfc0c0a671) 94

[NETLOGON\_INFO\_3 structure](#section_be92a2cd950c4b268cd3475065406b92) 95

[NETLOGON\_INFO\_4 structure](#section_a2b4c31118314de6bf5efe8427323144) 96

[NETLOGON\_INTERACTIVE\_INFO structure](#section_af76351fef6946bca451e4c4b99bac4a) 52

[NETLOGON\_LOGOFF\_UAS\_INFORMATION structure](#section_60f42175eff840cda0836ee43a64fcbd) 97

[NETLOGON\_LOGON\_IDENTITY\_INFO structure](#section_81c44fa00a2741b3b607de39cce7ea1d) 60

[NETLOGON\_LOGON\_INFO\_CLASS [Protocol]](#section_8c7808e54e5c420e9c9047286da2218f) 61

[NETLOGON\_LOGON\_INFO\_CLASS enumeration](#section_8c7808e54e5c420e9c9047286da2218f) 61

[NETLOGON\_LSA\_POLICY\_INFO structure](#section_4676ac8320994e33b680502fd8a32dbd) 41

[NETLOGON\_NETWORK\_INFO structure](#section_e17b03b8c1d243a198dbcf8d05b9c6a8) 53

[NETLOGON\_ONE\_DOMAIN\_INFO structure](#section_77cd977686124dab9748bfb07247fd4c) 45

[NETLOGON\_RENAME\_ALIAS structure](#section_15426b427d0740e4bca7933823d1b40e) 83

[NETLOGON\_RENAME\_GROUP structure](#section_c48a22162c51412baeb6c6666004b53f) 84

[NETLOGON\_RENAME\_USER structure](#section_96943cc2441245df8ac0f4b3d323a27e) 84

[NETLOGON\_SECURE\_CHANNEL\_TYPE [Protocol]](#section_4d1235e32c964e9fa1473cb338a0d09f) 48

[NETLOGON\_SECURE\_CHANNEL\_TYPE enumeration](#section_4d1235e32c964e9fa1473cb338a0d09f) 48

[NETLOGON\_SERVICE\_INFO structure](#section_1c9f2af2e16445489428eae68a03537e) 52

[NETLOGON\_SID\_AND\_ATTRIBUTES structure](#section_5454e6c6f78643278667d542b5ebb7c7) 54

[NETLOGON\_TRUSTED\_DOMAIN\_ARRAY structure](#section_251cf1be29324d338532595cf42e8091) 92

[NETLOGON\_VALIDATION\_GENERIC\_INFO2 structure](#section_e89f8f5b098541a0b1101ae0ea2bd183) 55

[NETLOGON\_VALIDATION\_INFO\_CLASS [Protocol]](#section_95154ae4d30543e582e4d5353e0f117c) 62

[NETLOGON\_VALIDATION\_INFO\_CLASS enumeration](#section_95154ae4d30543e582e4d5353e0f117c) 62

[NETLOGON\_VALIDATION\_SAM\_INFO structure](#section_142a277fe16145ac8b95b94bb169b5da) 56

[NETLOGON\_VALIDATION\_SAM\_INFO2 structure](#section_2a12e28979044ecb9d836732200230c0) 57

[NETLOGON\_VALIDATION\_SAM\_INFO4 structure](#section_bccfdba90c38485eb751d4de1935781d) 58

[NETLOGON\_VALIDATION\_UAS\_INFO structure](#section_7bd204f6aba3464cb02855e49f7999a0) 97

[NETLOGON\_WORKSTATION\_INFO structure](#section_3ae9e9a9a3034fa58e11823d9e7e1e61) 41

[NetrAccountDeltas method](#section_9a4ba74c00474053bd51d6204f291710) 215

[NetrAccountSync method](#section_717064350c2b4fd999abb27f28dc9ae0) 215

[NetrChainSetClientAttributes method](#section_3a416e8202994ff0a25d223f972ba1d6) 176

[NetrDatabaseDeltas method](#section_5412f0bc5eb94197b4c4c5a8c06ba018) 184

[NetrDatabaseRedo method](#section_c8352ce88b094baeaaf7456d7e6fda6c) 188

[NetrDatabaseSync method](#section_86683ada19a2414eafaf124f77dc4685) 188

[NetrDatabaseSync2 method](#section_31fc80bd4f4d4512a792e488bb78f6a0) 185

[NetrEnumerateTrustedDomains method](#section_1d106b28c30f4fd1b7b0240b6250d7f6) 193

[NetrEnumerateTrustedDomainsEx method](#section_c3e9870a09434d45be94edb9419a1c11) 192

[NetrGetAnyDCName method](#section_3db726ac0d1b43bebd6f923d97768436) 159

[NetrGetDCName method](#section_ddd7452f4b7d47e6895b5b23d9dd2120) 158

[NetrGetForestTrustInformation method](#section_63bab11ca90244a29cd7221357788483) 194

[NetrLogonComputeClientDigest method](#section_79ca6e90ccd2429eb5ac8050b620eef6) 203

[NetrLogonComputeServerDigest method](#section_5f95c374795142d9816cc7f4cff2ed52) 202

[NetrLogonControl method](#section_d62ebadc996749efa48db4059a7176c5) 214

[NetrLogonControl2 method](#section_650a105f64434eb0839a188708328fb0) 213

[NetrLogonControl2Ex method](#section_df7e5dd1ebcc47549da02e0bded82d29) 208

[NetrLogonGetCapabilities method](#section_5780fc6c82f0489fb9a0a9e855388492) 175

[NetrLogonGetDomainInfo method](#section_7c3ad0ccee054643b7734d84e1d431dc) 173

[NetrLogonGetTimeServiceParentDomain method](#section_be27686c237347439b655c97b2618bdd) 207

[NetrLogonGetTrustRid method](#section_1d6fad9e763d495f9bed18c79304c3d7) 201

[NetrLogonSamLogoff method](#section_a087dc875d4b40228f9156ac2dc20256) 182

[NetrLogonSamLogon method](#section_a3a192c800704ae3a537dfe0a144426a) 182

[Netrlogonsamlogon with secure channel example](#section_3c4678e3a52848fea9ed15b2319f7698) 223

[NetrLogonSamLogonEx method](#section_1725735133844de5bfe0453926ef67cd) 177

[NetrLogonSamLogonWithFlags method](#section_d17f1077de4b4fcd886739068cb789f5) 180

[NetrLogonSendToSam method](#section_b06e6b30fe574e0fba1a5214c953a5df) 204

[NetrLogonSetServiceBits method](#section_481bb1f8319a40fb89cdad1f6a146d9d) 205

[NetrLogonUasLogoff method](#section_f89840bc42154dc89d365c1e5fa6a77d) 214

[NetrLogonUasLogon method](#section_4db6051c9876446c957dc8f6aecbdb9a) 214

[NetrServerAuthenticate method](#section_2561f16011f943a7bad45721a05e8ad8) 168

[NetrServerAuthenticate2 method](#section_985982ae9aa84565b30b33d6353d3355) 167

[NetrServerAuthenticate3 method](#section_3a9ed16f801445ae80afc0ecb06e2db9) 165

[NetrServerGetTrustInfo method](#section_4c2296c3c6f047fc9f01a6fe17bf1d5b) 199

[NetrServerPasswordGet method](#section_5647a125f6ae4ea6acec14f3e9ec3a8b) 170

[NetrServerPasswordSet method](#section_a93310347f3047bd8aee93bbabe90df4) 169

[NetrServerPasswordSet2 method](#section_14b020a80bcf4af5ab72cc92bc6b1d81) 168

[NetrServerReqChallenge method](#section_5ad9db9f74414ce58c7b7b771e243d32) 165

[NetrServerTrustPasswordsGet method](#section_84b0d22a9b2c44328ae04a72eda28ea4) 172

[NL\_AUTH\_MESSAGE packet](#section_525f0bf3ebd943609343685767eb3c67) 37

NL\_AUTH\_MESSAGE token

[generate initial token](#section_d37cd1fb802f4d648f449bdb6adacc22) 114

[generation of return](#section_22973b64ea9440f49a65165bbdc4afaf) 115

[overview](#section_b28a01cb295d4833bdb6b113baf109b4) 114

[receipt of a return](#section_80447dc184844cae803606229cc9b281) 115

[receipt of initial token](#section_6f0201c33de94ea083b31634094be324) 115

[NL\_AUTH\_SHA2\_SIGNATURE packet](#section_fc77c8aa6c21446ba8224da26cc8a9a8) 39

[NL\_AUTH\_SIGNATURE packet](#section_05b99afd1b6a4207b16e959e6a483867) 38

[NL\_DNS\_NAME\_INFO structure](#section_1c7e652045a243e1ac0b43e771f85b14) 35

[NL\_DNS\_NAME\_INFO\_ARRAY structure](#section_8ae8a92eb63a43fd935097f1cab1c148) 37

[NL\_GENERIC\_RPC\_DATA structure](#section_a1c7f3cac8b145149fd5ed3460c83a4d) 92

[NL\_IN\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 structure](#section_f4ed8790d7e84ca18062d25784ed79e3) 50

[NL\_OSVERSIONINFO\_V1 structure](#section_98229ab4425a41d887ce48aacb302907) 49

[NL\_OUT\_CHAIN\_SET\_CLIENT\_ATTRIBUTES\_V1 structure](#section_ab43a76224e245c387011838589d80fe) 50

[NL\_PASSWORD\_VERSION structure](#section_cba0e87eb91f411b9be86fd321e126b7) 44

[NL\_SITE\_NAME\_ARRAY structure](#section_4c5fb44a6d68420d970e68ad5436bbd3) 33

[NL\_SITE\_NAME\_EX\_ARRAY structure](#section_2b40b2eb480c42e9b8643de716db892d) 33

[NL\_SOCKET\_ADDRESS structure](#section_235d0c09b9db44c59d4d806919be657b) 34

[NL\_TRUST\_PASSWORD structure](#section_52d5bd865caf47aaaae4cadf7339ec83) 43

[NLPR\_CR\_CIPHER\_VALUE structure](#section_c6fcb4974b1045958fe796bf961ba292) 80

[NLPR\_LOGON\_HOURS structure](#section_05a64da26e5f40cc9848700634100613) 74

[NLPR\_MODIFIED\_COUNT structure](#section_75dd36998abc45d29fb7e7a9a78779f5) 85

[NLPR\_QUOTA\_LIMITS structure](#section_55d7ea86c4cc4a5e8414426673cb77d1) 65

[NLPR\_SID\_ARRAY structure](#section_d89f92c6bc7c4af3a96d835e9ab03ca0) 69

[NLPR\_SID\_INFORMATION structure](#section_e936e7db27cb40ddacf7eec6ac0e9ed5) 69

[NLPR\_USER\_PRIVATE\_INFO structure](#section_1333d2308d174c16a09d0b7c785d591a) 74

[Normative references](#section_ae64d863ac764b6db00696d0669775b1) 18

[NT\_OWF\_PASSWORD structure](#section_f7458576d53847cdb387b6f98449a0ee) 30

O

Obsolete methods ([section 3.4.5.8](#section_c96e78b25b964002bf2f3d6297736edc) 136, [section 3.5.4.10](#section_a9dccfcfea6e4f919c0739183708e34e) 214)

[Obsolete Methods method](#section_a9dccfcfea6e4f919c0739183708e34e) 214

[Obsolete structures](#section_7a86a6835c4a4a71b0659c73f6c1beb8) 97

[Overview (synopsis)](#section_70d9e96a9e32432188334b597efc87a7) 20

P

[Parameters - security index](#section_d1369c2670ce4c768a29f10cccead4a5) 231

Pass-through authentication ([section 1.3.1](#section_70697480f28548369ca77bb52f18c6af) 20, [section 1.3.2](#section_08b36439331a4e2089a512f3fab33dfc) 21)

[abstract data model](#section_1875a45ababe4ab4a4c26abe02ab6858) 112

[initialization](#section_2c9e1afa6b4d4101ac5f1fe325c213fe) 112

[local events](#section_675e0368a23f475196503b29a329bcc8) 113

[message processing](#section_785693dfc2484c4596cab17c1a365a9b) 112

[overview](#section_8ea3ca7111074888b108f5bdcb350eea) 111

[sequencing rules](#section_785693dfc2484c4596cab17c1a365a9b) 112

[timer events](#section_9a0d4289efec4470a1f59edac0568db0) 113

[timers](#section_2d92a5b6a4f24ac4a63583f8c079f252) 112

Pass-through authentication methods ([section 3.4.5.3](#section_c3eda426dd4f494f8c3a97c0aa479cc9) 129, [section 3.5.4.5](#section_24933c92b96540f19e1d74ea27d4813c) 177, [section 3.5.4.6](#section_5657e68eab5b4d9998b80fcaa1bdffc6) 184)

Pass-Through Authentication Methods method ([section 3.4.5.3](#section_c3eda426dd4f494f8c3a97c0aa479cc9) 129, [section 3.5.4.5](#section_24933c92b96540f19e1d74ea27d4813c) 177)

[Pass-through authentication structures](#section_d76f87d0b8a142e8b3b147ab47444cbc) 51

[PCYPHER\_BLOCK](#section_56a8d298dbeb4eb5ad9876536ec352f8) 29

[PDOMAIN\_CONTROLLER\_INFOW](#section_9b85a7a48d344b9e9500bf8644ebfc06) 31

[PDOMAIN\_NAME\_BUFFER](#section_11743dc47a2d4464b35150aeb8801b8b) 89

[PDS\_DOMAIN\_TRUSTSW](#section_7de9866ed3ef4a9f98a5c2dcff1e61c1) 89

[PENCRYPTED\_LM\_OWF\_PASSWORD](#section_30a12be7a4ed4ef2bd8883961edb8f26) 30

[PENCRYPTED\_NT\_OWF\_PASSWORD](#section_f7458576d53847cdb387b6f98449a0ee) 30

[PGROUP\_MEMBERSHIP](#section_efb926f648c34c298a4586a67bfaaf27) 55

[PLM\_OWF\_PASSWORD](#section_30a12be7a4ed4ef2bd8883961edb8f26) 30

[PNETLOGON\_AUTHENTICATOR](#section_76c93227942a4687ab9d9d972ffabdab) 31

[PNETLOGON\_CREDENTIAL](#section_d55e263271634f6cb6624b870e8cc1cd) 41

[PNETLOGON\_DELTA\_ACCOUNTS](#section_7f60a1a799d849ba91c06e027237b009) 66

[PNETLOGON\_DELTA\_ALIAS](#section_38155d03b5dc445d9fcba6938be5972d) 68

[PNETLOGON\_DELTA\_ALIAS\_MEMBER](#section_aeca74675e13417ca4cb71d1f6476090) 69

[PNETLOGON\_DELTA\_DELETE\_GROUP](#section_3ef0689005194f6e889dec76cd865d7c) 70

[PNETLOGON\_DELTA\_DELETE\_USER](#section_3fb60f5fe33d427bb540ac3b84342d5d) 70

[PNETLOGON\_DELTA\_DOMAIN](#section_803be876d7554187a011eaf5bf2755ab) 71

[PNETLOGON\_DELTA\_ENUM](#section_20e5863c014240f6a914f352a9d66047) 72

[PNETLOGON\_DELTA\_ENUM\_ARRAY](#section_82d47318c4d8458386a6ce186504bcba) 72

[PNETLOGON\_DELTA\_GROUP](#section_b7949b4e0fc740d488418d69230e2d79) 73

[PNETLOGON\_DELTA\_GROUP\_MEMBER](#section_3d4c56361f2a4896a717d8598ffaffab) 78

[PNETLOGON\_DELTA\_POLICY](#section_b9ee3608efd14d57b4da5a13b9ec1fa1) 79

[PNETLOGON\_DELTA\_RENAME\_ALIAS](#section_15426b427d0740e4bca7933823d1b40e) 83

[PNETLOGON\_DELTA\_RENAME\_GROUP](#section_c48a22162c51412baeb6c6666004b53f) 84

[PNETLOGON\_DELTA\_RENAME\_USER](#section_96943cc2441245df8ac0f4b3d323a27e) 84

[PNETLOGON\_DELTA\_SECRET](#section_ddf4e131ef89425fa70b88fdd73afb51) 81

[PNETLOGON\_DELTA\_TRUSTED\_DOMAINS](#section_fe95340edb884fdd85c6bc8ad1c4ff8c) 82

[PNETLOGON\_DELTA\_USER](#section_c82fcc5a59b647f79f69dec916ebed2c) 77

[PNETLOGON\_DOMAIN\_INFO](#section_440c3430ed5f481db60274db422df3c8) 46

[PNETLOGON\_GENERIC\_INFO](#section_c03d6d959b5e43299645eedcdd167f6e) 51

[PNETLOGON\_INFO\_1](#section_afeb873c48264beba35cae73a708b108) 93

[PNETLOGON\_INFO\_2](#section_c48a87004c174afb8866f0cfc0c0a671) 94

[PNETLOGON\_INFO\_3](#section_be92a2cd950c4b268cd3475065406b92) 95

[PNETLOGON\_INFO\_4](#section_a2b4c31118314de6bf5efe8427323144) 96

[PNETLOGON\_INTERACTIVE\_INFO](#section_af76351fef6946bca451e4c4b99bac4a) 52

[PNETLOGON\_LOGOFF\_UAS\_INFO](#section_60f42175eff840cda0836ee43a64fcbd) 97

[PNETLOGON\_LOGON\_IDENTITY\_INFO](#section_81c44fa00a2741b3b607de39cce7ea1d) 60

[PNETLOGON\_LSA\_POLICY\_INFO](#section_4676ac8320994e33b680502fd8a32dbd) 41

[PNETLOGON\_NETWORK\_INFO](#section_e17b03b8c1d243a198dbcf8d05b9c6a8) 53

[PNETLOGON\_ONE\_DOMAIN\_INFO](#section_77cd977686124dab9748bfb07247fd4c) 45

[PNETLOGON\_SERVICE\_INFO](#section_1c9f2af2e16445489428eae68a03537e) 52

[PNETLOGON\_SID\_AND\_ATTRIBUTES](#section_5454e6c6f78643278667d542b5ebb7c7) 54

[PNETLOGON\_TRUSTED\_DOMAIN\_ARRAY](#section_251cf1be29324d338532595cf42e8091) 92

[PNETLOGON\_VALIDATION\_GENERIC\_INFO2](#section_e89f8f5b098541a0b1101ae0ea2bd183) 55

[PNETLOGON\_VALIDATION\_SAM\_INFO](#section_142a277fe16145ac8b95b94bb169b5da) 56

[PNETLOGON\_VALIDATION\_SAM\_INFO2](#section_2a12e28979044ecb9d836732200230c0) 57

[PNETLOGON\_VALIDATION\_SAM\_INFO4](#section_bccfdba90c38485eb751d4de1935781d) 58

[PNETLOGON\_VALIDATION\_UAS\_INFO](#section_7bd204f6aba3464cb02855e49f7999a0) 97

[PNETLOGON\_WORKSTATION\_INFO](#section_3ae9e9a9a3034fa58e11823d9e7e1e61) 41

[PNL\_DNS\_NAME\_INFO](#section_1c7e652045a243e1ac0b43e771f85b14) 35

[PNL\_DNS\_NAME\_INFO\_ARRAY](#section_8ae8a92eb63a43fd935097f1cab1c148) 37

[PNL\_GENERIC\_RPC\_DATA](#section_a1c7f3cac8b145149fd5ed3460c83a4d) 92

[PNL\_PASSWORD\_VERSION](#section_cba0e87eb91f411b9be86fd321e126b7) 44

[PNL\_SITE\_NAME\_ARRAY](#section_4c5fb44a6d68420d970e68ad5436bbd3) 33

[PNL\_SITE\_NAME\_EX\_ARRAY](#section_2b40b2eb480c42e9b8643de716db892d) 33

[PNL\_SOCKET\_ADDRESS](#section_235d0c09b9db44c59d4d806919be657b) 34

[PNL\_TRUST\_PASSWORD](#section_52d5bd865caf47aaaae4cadf7339ec83) 43

[PNLPR\_CR\_CIPHER\_VALUE](#section_c6fcb4974b1045958fe796bf961ba292) 80

[PNLPR\_LOGON\_HOURS](#section_05a64da26e5f40cc9848700634100613) 74

[PNLPR\_MODIFIED\_COUNT](#section_75dd36998abc45d29fb7e7a9a78779f5) 85

[PNLPR\_QUOTA\_LIMITS](#section_55d7ea86c4cc4a5e8414426673cb77d1) 65

[PNLPR\_SID\_ARRAY](#section_d89f92c6bc7c4af3a96d835e9ab03ca0) 69

[PNLPR\_SID\_INFORMATION](#section_e936e7db27cb40ddacf7eec6ac0e9ed5) 69

[PNLPR\_USER\_PRIVATE\_INFO](#section_1333d2308d174c16a09d0b7c785d591a) 74

[PNT\_OWF\_PASSWORD](#section_f7458576d53847cdb387b6f98449a0ee) 30

[Preconditions](#section_41679899e81b41bfaddae269ce9dc33d) 27

[Prerequisites](#section_41679899e81b41bfaddae269ce9dc33d) 27

[Product behavior](#section_0c858a52732a43ec85dde44b357c1898) 256

Protocol Details

[overview](#section_2d776bfce81f4c8f9da84c2920f65413) 99

[PSTRING](#section_4a896c09a39c487894f09e4f8a419f32) 30

[PUAS\_INFO\_0](#section_5140443cef1e48e8b9c715d34cb91423) 97

[PUSER\_SESSION\_KEY](#section_9c07428ca9074590a2c1bb95a009e527) 55

R

[References](#section_2fa21ab324e04d259f219a0aeee11f5f) 17

[informative](#section_e5df11eeeefe4fc295bd489e86f22292) 19

[normative](#section_ae64d863ac764b6db00696d0669775b1) 18

[Relationship to other protocols](#section_7a24669b2afa4b1388730a7a2686cfff) 26

[Replication - account database](#section_7afa81d37f3e4dc2990a901d7fec94d3) 22

[RPC binding handles](#section_3b224201b53143e28c79b61f6dea8640) 146

[RPC Binding Handles for Netlogon Methods method](#section_3b224201b53143e28c79b61f6dea8640) 146

S

[Schema elements - directory service](#section_6e72c5303cc14f0d9a71b3df690721ee) 98

Secure channel establishment and maintenance methods ([section 3.4.5.2](#section_b340eff0540a47a7ad491706d4b72a8b) 125, [section 3.5.4.4](#section_641f684e080943f38ba92a3754874126) 164)

[Secure Channel Establishment and Maintenance Methods method](#section_641f684e080943f38ba92a3754874126) 164

[Secure channel establishment and maintenance structures](#section_fb50db727f71478da18012eb0ca3b36b) 37

[Secure channel maintenance](#section_f1c87149fc1d492a883d33cfc624dce4) 23

Security

[implementer considerations](#section_0b6a8035850e4b1195cd1717ed2516fe) 230

[parameter index](#section_d1369c2670ce4c768a29f10cccead4a5) 231

Sequencing rules

[client](#section_63e975f1e219416e96c4ee2a30bf73b0) 124

[Netlogon as security support provider](#section_eaa58b8aae4941bc9c91846d7746535f) 114

[Netlogon common authentication](#section_f4d97830929947c2b0cdb1da9dec520a) 102

Netlogon NT replication ([section 3.6.4](#section_f310867bca064d37addff7dcd9f97ad7) 218, [section 3.6.4.1](#section_724235138903472f865c7b12ade645f4) 218)

[pass-through authentication](#section_785693dfc2484c4596cab17c1a365a9b) 112

[server](#section_256678803d51499bb22819c08eb16b81) 141

Server

[abstract data model](#section_b8d168acebb642f4bfb27a84377f2cbc) 137

[Account Database Replication Methods method](#section_5657e68eab5b4d9998b80fcaa1bdffc6) 184

[Administrative Services Methods method](#section_647e0ebb338f499fabbc8f82adcb36ff) 208

[DC Location Methods method](#section_2c26616cfe894d0288aea56356e0f512) 147

[Determining client privileges method](#section_1ec948862b6445afb68e3d9faa36617c) 147

[Domain Trust Methods method](#section_d6ee9b3a1cf24719a82773f2e0298336) 190

[initialization](#section_f8c12682fd984c1a8b0ab6e153f96186) 140

[local events](#section_4d79a456cd4e4474ae9c60d2143a0e57) 215

[message processing](#section_256678803d51499bb22819c08eb16b81) 141

[Message Protection Methods method](#section_fff9e47b029f41e0b48b1f5c5554b68f) 201

[Obsolete Methods method](#section_a9dccfcfea6e4f919c0739183708e34e) 214

[Pass-Through Authentication Methods method](#section_24933c92b96540f19e1d74ea27d4813c) 177

[RPC Binding Handles for Netlogon Methods method](#section_3b224201b53143e28c79b61f6dea8640) 146

[Secure Channel Establishment and Maintenance Methods method](#section_641f684e080943f38ba92a3754874126) 164

[sequencing rules](#section_256678803d51499bb22819c08eb16b81) 141

[timer events](#section_8bcabeb0ac8f48a9a5c9fa5e968eae88) 215

[timers](#section_b27ea0ae8c4e4af2bf0cca5382290e7d) 140

[Session-key computation](#section_5e9798475b2a4148b6e9047c65a8ae63) 106

[Session-key negotiation](#section_7b9e31d1670e4fc5ad549ffff50755f9) 102

[Standards assignments](#section_c892ce41af4e4a44b2ebb76666ae4863) 28

[STRING structure](#section_4a896c09a39c487894f09e4f8a419f32) 30

Structures

[account database replication](#section_c4adbfb3678b4996860f3602709558b9) 63

[administrative services structures](#section_3b7ad20ab8c64191971e8b96f85d0899) 92

[basic structures](#section_5fc4156477124f478ca634edc1721bae) 29

[DC location structure](#section_94c3b27ad8064eacbfe15a48e63eeca9) 31

[domain trust structures](#section_26bc3213bff74ed5ac5b651bab12d874) 89

[obsolete](#section_7a86a6835c4a4a71b0659c73f6c1beb8) 97

[overview](#section_c3a0defffd1b4df9850f420cb8a224f5) 29

[pass-through authentication structures](#section_d76f87d0b8a142e8b3b147ab47444cbc) 51

[secure channel establishment and maintenance structures](#section_fb50db727f71478da18012eb0ca3b36b) 37

[Structures - Netlogon](#section_a1aa6492171b49cbaf4e991c7461cf56) 24

[SYNC\_STATE [Protocol]](#section_ffce9bbc6ae544788f45e82c3847aaa2) 88

[SYNC\_STATE enumeration](#section_ffce9bbc6ae544788f45e82c3847aaa2) 88

T

Timer events

[Netlogon as security support provider](#section_06fe5d6862b445ed9dc7f8188ac6872d) 121

Netlogon common authentication ([section 3.1.5](#section_0a9c7006b77e4a979660878df7d9966c) 111, [section 3.1.6](#section_6e9975e7c21d4ec5aafc0dfdf7325ebe) 111)

Netlogon NT replication ([section 3.6.5](#section_202c7366b4974c3a914ff8ff35047b90) 220, [section 3.6.5.1](#section_ce890453cb5a4e999a16f56c7c3e9eca) 220)

[pass-through authentication](#section_9a0d4289efec4470a1f59edac0568db0) 113

[server](#section_8bcabeb0ac8f48a9a5c9fa5e968eae88) 215

Timers

[client](#section_b9ebbb2e8e894db98a9beab526d5e0ca) 123

[Netlogon as security support provider](#section_acdc3f370ba8486fbbc08aa4ff254286) 114

[Netlogon common authentication](#section_b1bf5a578cf44ceaa792adeec3bc87c4) 102

[Netlogon NT replication](#section_6454b09273ec4b02b5d2454655cfed6a) 218

Pass-through authentication ([section 3.2.2](#section_2d92a5b6a4f24ac4a63583f8c079f252) 112, [section 3.2.3](#section_2c9e1afa6b4d4101ac5f1fe325c213fe) 112)

[server](#section_b27ea0ae8c4e4af2bf0cca5382290e7d) 140

[Tracking changes](#section_62cbfaee898d465bb44cf380deeb696b) 276

[Transport](#section_592edbc8f6f140c09ab3fe6725ac6d7e) 29

[Triggered events - higher-layer - client](#section_41344b38080b4a55afa2e45997273a80) 124

[Trust - domain - structures](#section_26bc3213bff74ed5ac5b651bab12d874) 89

Trusts - domain ([section 1.3.2](#section_08b36439331a4e2089a512f3fab33dfc) 21, [section 1.3.5](#section_a7aa8f241cac469b8671ef6c7d31d5e5) 23)

U

[UAS\_INFO\_0 structure](#section_5140443cef1e48e8b9c715d34cb91423) 97

[USER\_SESSION\_KEY structure](#section_9c07428ca9074590a2c1bb95a009e527) 55

V

[Vendor-extensible fields](#section_75eb779b284b47d78aa1069ad71928a7) 28

[Versioning](#section_b5ad98b323be467e91cda580aab8abaf) 27