Windows Protocols Errata

This topic lists the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata are content issues in published versions of protocols documents that could impact an **implementation**. Examples of errata are errors or missing information in the normative sections of the Technical Specifications or in the use cases (examples) in the Technical Specifications and Overview Documents.

Content issues that don't impact an implementation, for example, editorial updates due to typos, formatting updates, and rewrites for readability and clarity, are **not** included in Errata.

The sections below list the Windows Protocols documents that contain active Errata (i.e., Errata not yet released with the documents on Docs.Microsoft.Com [DMC]) and provide links to archived Errata (i.e., Errata already released with the documents on DMC).

Protocols Documents with Active Errata

[MC-NBFX]: .NET Binary Format: XML Data Structure

[MC-NMF]: .NET Message Framing Protocol

[MS-ADSC]: Active Directory Schema Classes

[MS-CIFS]: Common Internet File System (CIFS) Protocol

[MS-CRTD]: Certificate Templates Structure

[MS-CSSP]: Credential Security Support Provider (CredSSP) Protocol

[MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol

[MS-DNSP]: Domain Name Service (DNS) Server Management Protocol

[MS-DRSR]: Directory Replication Service (DRS) Remote Protocol

[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

[MS-EVEN]: EventLog Remoting Protocol

[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

[MS-FSA]: File System Algorithms

[MS-FSCC]: File System Control Codes

[MS-KILE]: Kerberos Protocol Extensions

[MS-LCID]: Windows Language Code Identifier (LCID) Reference

[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol

[MS-MDE2]: Mobile Device Enrollment Protocol Version 2

[MS-MDM]: Mobile Device Management Protocol

[MS-NNS]: .NET NegotiateStream Protocol

[MS-NRBF]: .NET Remoting: Binary Format Data Structure

[MS-NRPC]: Netlogon Remote Protocol

[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

[MS-RDPEAR]: Remote Desktop Protocol Authentication Redirection Virtual Channel

[MS-RDPECLIP]: Remote Desktop Protocol Clipboard Virtual Channel Extension

[MS-RDPEUDP2]: Remote Desktop Protocol UDP Transport Extension Version 2

[MS-RNAS]: Vendor-Specific RADIUS Attributes for Network Policy and Access Server (NPAS) Data Structure

[MS-SFU]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol

[MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3

[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)

[MS-SSTR]: Smooth Streaming Protocol

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

[MS-WKST]: Workstation Service Remote Protocol

[MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions[

[MS-WUSP]: Windows Update Services Client-Server Protocol

Errata Archives

June 30, 2015 - Download

October 16, 2015 - Download

March 2, 2016 - Download

July 18, 2016 - Download

September 26, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

August 21, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

June 24, 2019 – Download

September 23, 2019 - Download

October 14, 2019 - Download

March 4, 2020 - Download

June 15, 2020 - Download

August 24, 2020 – Download

September 29, 2020 – Download

November 23, 2020 - Download

April 7, 2021 - Download

June 1, 2021 - Download

June 24, 2021 - Download

October 6, 2021 - Download

May 2, 2022 - Download

[MC-DTCXA]: MSDTC Connection Manager OleTx XA Protocol

This topic lists the Errata found in [MC-DTCXA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MC-NBFX]: .NET Binary Format XML Data Structure

This topic lists the Errata found in [MC-NBFX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2019/03/13.

Errata Published*	Description
2019/12/09	In Section 2.2.3.30, QNameDictionaryTextRecord(0xBC), the length of the Name field was changed from 3 bytes to variable: Changed from: Name (3 bytes) Changed to: Name (variable) The packet diagram for the message was also changed to reflect the length.

*Date format: YYYY/MM/DD

[MC-NMF]: .NET Message Framing Protocol

This topic lists the Errata found in the MC-NMF document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V9.0 – 2018/03/16.

Errata Published*	Description
2018/07/02	In Section 2.2.6, Preamble Message, the field descriptions have been modified as follows and have been moved to follow the packet diagram. Changed from: The VersionRecord MUST be formatted as specified in section 2.2.3.1. The ModeRecord MUST be formatted as specified in section 2.2.3.2. The ViaRecord MUST be formatted as specified in section 2.2.3.3. The EnvelopeEncodingRecord MUST be formatted as specified in section 2.2.3.4 Changed to: VersionRecord (3 bytes): This field MUST be formatted as specified in section 2.2.3.1. ModeRecord (2 bytes): This field MUST be formatted as specified in section 2.2.3.2. ViaRecord (variable): This field MUST be formatted as specified in section 2.2.3.3. EnvelopeEncodingRecord (variable): This field MUST be formatted as specified in section 2.2.3.4

*Date format: YYYY/MM/DD

[MC-PRCR]: Peer Channel Custom Resolver Protocol

This topic lists the Errata found in [MC-PRCR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 15, 2017 - Download

[MS-ABTP]: Automatic Bluetooth Pairing Protocol

This topic lists the Errata found in [MS-ABTP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ADA2]: Active Directory Schema Attributes M

This topic lists the Errata found in the MS-ADA2 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

[MS-ADA3]: Active Directory Schema Attributes N-Z

This topic lists the Errata found in the MS-ADA3 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-ADDM]: Active Directory Web Services: Data Model and Common Elements

This topic lists the Errata found in [MS-ADDM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

[MS-ADFSOAL]: Active Directory Federation Services OAuth Authorization Code Lookup Protocol

This topic lists the Errata found in [MS-ADFSOAL] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-ADFSPIP]: Active Directory Federation Services and Proxy Integration Protocol

This topic lists the Errata found in the MS-ADFSPIP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 30, 2015 - Download

July 18, 2016 - Download

September 15, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

[MS-ADFSWAP]: Active Directory Federation Service (AD FS) Web Agent Protocol

This topic lists the Errata found in [MS-ADFSWAP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

[MS-ADLS]: Active Directory Lightweight Directory Services Schema

This topic lists the Errata found in the MS-ADLS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-ADSC]: Active Directory Schema Classes

This topic lists the Errata found in the MS-ADSC document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V23.0 – 2018/03/16.

Errata Published*	Description

2019/09/16	In Section 2.243, Class samDomain, changed from:
	
	`(OA;CIOI;RPWP;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;PS)`
	`S:(AU;SA;WDWOWP;;;WD)(AU;SA;CR;;;BA)(AU;SA;CR;;;DU)`
	
	Changed to:
	
	`(OA;CIOI;RPWP;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;PS)`
	`(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;PS)`
	`(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;CO)`
	`S:(AU;SA;WDWOWP;;;WD)(AU;SA;CR;;;BA)(AU;SA;CR;;;DU)`

*Date format: YYYY/MM/DD

[MS-ADTS]: Active Directory Technical Specification

This topic lists the Errata found in the MS-ADTS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

[MS-AIPS]: Authenticated Internet Protocol

This topic lists the Errata found in the MS-AIPS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-APDS]: Authentication Protocol Domain Support

This topic lists the Errata found in the MS-APDS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-AZOD]: Authorization Protocols Overview

This topic lists the Errata found in the MS-AZOD document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2021 - Download

[MS-BKRP]: BackupKey Remote Protocol

This topic lists the Errata found in the MS-BKRP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V24.0 - 2021/06/25.

Errata Published*	Description
2022/01/11	The following sections were changed. Please see the diff document for the details. In Section 3.2.4.1 Performing Client-Side Wrapping of Secrets, Product Behavior Note<18> Description: Revised to disable the data protection API master key backup fallback by default, as the use of the RC4 algorithm to back up the data protection API master key is no longer available by default. Changed from: Windows XP operating system and later and Windows Server 2003 operating system and later fall back to server-side wrapping using BACKUPKEY_BACKUP_GUID when they fail to retrieve the server's public key using BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID. In addition, as noted earlier, Windows clients always retry failing operations once. The resulting process is as follows: The client first tries the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID operation and, if it fails, performs DC rediscovery and retries the same operation. If the retry fails, the client tries a BACKUPKEY_BACKUP_GUID operation. If this fails, the client performs DC rediscovery again and retries the BACKUPKEY_BACKUP_GUID operation. If this also fails, an error is returned to the caller. Changed to: The process of falling back to server-side wrapping using the BACKUPKEY_BACKUP_GUID when retrieval of the server's public key fails using the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID is no longer available by default for the operating systems specified in [MSFT-CVE-2022-21925]. However, the fall back can be enabled by adding a registry key designed for this purpose. In addition, as noted earlier, Windows clients always retry failing operations once. The resulting process is as follows: The client first tries the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID operation, and if it fails, the client performs DC rediscovery and retries the same operation. If the retry fails, the client tries a BACKUPKEY_BACKUP_GUID operation. If this fails, the client performs DC rediscovery again and retries the BACKUPKEY_BACKUP_GUID operation. If this also fails, an error is returned to the caller.

[MS-BKUP]: Microsoft NT Backup File Structure

This topic lists the Errata found in the MS-BKUP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-CAPR]: Central Access Policy Identifier (ID) Retrieval Protocol

This topic lists the Errata found in the MS-CAPR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-CDP]: Connected Devices Platform Protocol Version 3

This topic lists the Errata found in the MS-CDP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

April 29, 2022 - Download

[MS-CHAP]: Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP)

This topic lists the Errata found in the MS-CHAP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-CFB]: Compound File Binary File Format

This topic lists the Errata found in the MS-CFB document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

March 16, 2018 - Download

[MS-CIFS]: Common Internet File System (CIFS) Protocol

This topic lists the Errata found in the MS-CIFS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 4, 2020 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V30.0 - 2020/10/01

Errata Published*	Description
2021/01/11	In Section 6 Appendix A: Product Behavior, the following behavior notes have been updated: Changed from: <245> Section 3.3.5.5 ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see below) • For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped

Errata Published*	Description
	to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM, "COM". All other file names are mapped to SharingMode 3. ● For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed to: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE ● For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM, "COM". All other file names are mapped to SharingMode 3. ● If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed from: <297> Section 3.3.5.35 ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ

Errata Published*	Description
	3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see below) ● For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", and "COM". All other file names are mapped to SharingMode 3. ● For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed to: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE ● For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", and "COM". All other file names are mapped to SharingMode 3. ● If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed from: <339> Section 3.3.5.58.2 ...

Errata Published*	Description
	AccessMode.SharingMode ShareAccess 0 Compatibility mode (see following) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see following) ● For Compatibility mode, special filename suffixes (after the "." in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", "COM". All other file names are mapped to SharingMode 3. ● For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed To: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see following) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE ● For Compatibility mode, special filename suffixes (after the "." in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", "COM". All other file names are mapped to SharingMode 3. ● If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1.

Errata Published*	Description
	…

*Date format: YYYY/MM/DD

[MS-CMRP]: Failover Cluster: Management API (ClusAPI) Protocol

This topic lists the Errata found in the MS-CMRP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 29, 2022 - Download

[MS-COMA]: Component Object Model Plus (COMplus) Remote Administration Protocol

This topic lists the Errata found in the MS-COMA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-CRTD]: Certificate Templates Structure

This topic lists the Errata found in [MS-CRTD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

Errata below are for Protocol Document Version V26.0 – 2021/06/25.

Errata Published*	Description
2022/06/28	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA.
2022/06/14	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA."</td></tr>
<tr><td>2022/05/10</td><td>Section 2.26 msPKI-Enrollment-Flag Attribute

Description: "Added the CT_FLAG_NO_SECURITY_EXTENSION (0x00080000) enrollment flag that instructs the CA to not include security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2) in the issued certificate. Also added operating system applicability [MSFT-CVE-2022-26931] for this security update."

Changed From:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
</table>

Changed To:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
<tr><td>0x00080000
CT_FLAG_NO_SECURITY_EXTENSION</td><td>This flag[34] instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate.</td></tr>
</table>

[34] This flag is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed.</td></tr>
<tr><td>2021/07/27</td><td>In Section 2.27 msPKI-Private-Key-Flag Attribute, replaced normative reference [PKCS12] with [RFC7292].

Changed from:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00000010
CT_FLAG_EXPORTABLE_KEY</td><td>This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [PKCS12], at a later time.</td></tr>
</table>

Changed to:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
</table>
</td></tr>
</table>

Errata Published*	Description	
	0x00000010 CT_FLAG_EXPORTABLE_KEY	This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [RFC7292], at a later time.

*Date format: YYYY/MM/DD

[MS-CSRA]: Certificate Services Remote Administration Protocol

This topic lists the Errata found in the MS-CSRA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 12, 2018 - Download

September 29, 2020 – Download

[MS-CSSP]: Credential Security Support Provider (CredSSP) Protocol

This topic lists the Errata found in the MS-CSSP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V20.0 – 2021/06/25.

Errata Published*	Description
2021/09/07	In Section 2.2.1.2.3.1 TSRemoteGuardPackageCred, changed credBuffer: Windows CredSSP usage of Kerberos User to User tickets. Changed from: credBuffer: An ASN.1 OCTET STRING byte buffer that contains the credentials in a format that SHOULD<22> be specified by the CredSSP server operating system for the package that provided them. <22> Section 2.2.1.2.3.1: . . .Windows CredSSP clients will use Kerberos User to User tickets ([RFC4120], section 2.9.2) as the ServiceTicket, but the server does not enforce this. . . Changed to: credBuffer: An ASN.1 OCTET STRING byte buffer that contains the credentials in a format that SHOULD<22> be specified by the CredSSP server operating system for the package that provided them. <22> Section 2.2.1.2.3.1: . . .Windows CredSSP clients do not use Kerberos User to User tickets ([RFC4120], section 2.9.2) as the ServiceTicket, but can if necessary; the server does not enforce this. . .
2021/08/10	In Section 2.2.1.2.3.1 TSRemoteGuardPackageCred, adjusted supplemental credential code arrangement and added C bit flag for the Credential Key being present. Changed from: typedef struct _NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL { ULONG Version;

Errata Published*	Description
	ULONG Flags; MSV1_0_CREDENTIAL_KEY_TYPE reserved; MSV1_0_CREDENTIAL_KEY reserved; ULONG reservedsize; [size_is(reservedSize)] UCHAR* reserved; } NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL; Version: A 32-bit unsigned integer that defines the credential version. This field is 0xFFFF0002. Flags: A 32-bit unsigned integer containing flags that define the credential options. At least one of the following values is required. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 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 N L Where the bits are defined as follows: Value: Description L: Indicates that the LM OWF member is present and valid. N: Indicates that the NT OWF member is present and valid. Changed to: typedef struct _NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL { ULONG Version; ULONG Flags; MSV1_0_CREDENTIAL_KEY reserved; MSV1_0_CREDENTIAL_KEY_TYPE reserved; ULONG reservedsize; [size_is(reservedSize)] UCHAR* reserved; } NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL; Version: A 32-bit unsigned integer that defines the credential version. This field is 0xFFFF0002. Flags: A 32-bit unsigned integer containing flags that define the credential options. At least one of the following values is required. 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 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 0 N L Where the bits are defined as follows: Value: Description

Errata Published*	Description
	<table><tr><td>L</td><td>Indicates that the LM OWF member is present and valid.</td></tr><tr><td>N</td><td>Indicates that the NT OWF member is present and valid.</td></tr><tr><td>C</td><td>Indicates that the reserved credential key is present and valid ([MS-RDPEAR] section 2.2.1.3.5).</td></tr></table>

*Date format: YYYY/MM/DD

[MS-CSVP]: Failover Cluster: Setup and Validation Protocol (ClusPrep)

This topic lists the Errata found in the MS-CSVP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

August 24, 2020 – Download

[MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol

This topic lists the Errata found in the MS-DCOM document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version 23.0 - 2021/06/25.

Errata Published*	Description
2022/11/07	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Specified that the Windows 11 v22H2 operating system supports this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as

Errata Published*	Description
	applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system, Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related KB article download installed: Windows 11 (Sun Valley) Desktop, Windows 11 (Sun Valley) Desktop Refresh, Windows 11 Desktop v22H2, Windows Server 2022 - Full/Core, Windows 10 Desktop v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.
2022/10/24	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Also specified the operating systems that support this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. <pbn-80>Updated; see below. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system,

Errata Published*	Description
	Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related KB article download installed: Windows 11, Windows 11 Refresh, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server v1809 operating system, Windows Server 2012 R2, Windows Server 2012 operating system, Windows Server 2008 operating system with Service Pack 2 (SP2), Windows 10 version 22H2 operating system, Windows 10 v21H2 operating system, Windows 10 v21H1 operating system, Windows 10 v20H2 operating system, Windows 10 v1809 operating system, Windows 10 v1909 operating system, Windows 10 v1607 operating system, Windows 10 v1507 operating system, and Windows 7 operating system with Service Pack 1 (SP1).
2022/10/11	In Section 2.2.22.2.8.1 customREMOTE_REPLY_SCM_INFO Description: Updated product behavior note 37 in section 2.2.22.2.8.1 to ensure that RPC_C_AUTHN_LEVEL_PKT_INTEGRITY authentication level will be the minimum auth level following evaluation of the authentication level of DCOM client calls. Also specified the operating systems that support this behavior. Changed from: <37> Section 2.2.22.2.8.1: On Windows, DCOM servers return an RPC authentication level that denotes the minimum authentication level at which the object exporter can be called. On Windows, DCOM clients make calls to object exporters at an authentication level that is at least as high as the authnHint returned from the object server. Changed to: <37> Section 2.2.22.2.8.1: On Windows, DCOM servers return an RPC authentication level that denotes the minimum authentication level at which the object exporter can be called. On Windows, DCOM clients make calls to object exporters at an authentication level that is at least as high as the authnHint value returned from the object server, or the RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level, whichever is greater. Including the RPC_C_AUTHN_LEVEL_PKT_INTEGRITY authentication level in this evaluation is supported by the operating systems specified in [MSFT-CVE-2022-37978], each with its related KB article download installed.
2022/10/04	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Also specified the operating systems that support this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-

Errata Published*	Description
	specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. <pbn-80>Updated; see below. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system, Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related KB article download installed: Windows 11 (Sun Valley) Desktop, Windows 11 (Sun Valley) Desktop Refresh, Windows Server 2022 - Full/Core, Windows 10 Desktop v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.

[MS-DFSC]: Distributed File System (DFS) Referral Protocol

This topic lists the Errata found in [MS-DFSC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

[MS-DHCPE]: Dynamic Host Configuration Protocol (DHCP) Extensions

This topic lists the Errata found in [MS-DHCPE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-DHCPM]: Microsoft Dynamic Host Configuration Protocol (DHCP) Server Management Protocol

This topic lists the Errata found in [MS-DHCPM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

September 15, 2017 - Download

[MS-DNSP]: Domain Name Service (DNS) Server Management Protocol

This topic lists the Errata found in the MS-DNSP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 12, 2018 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V37.0 – 2021/04/07.

Errata Published*	Description
2021/08/17	In Section 3.1.4.5 R_DnssrvUpdateRecord (opnum 4), added processing behavior for the static condition. Changed from: • If the pAddRecord is for an explicitly defined resource record type DNS_TYPE_CNAME (section 2.2.2.1.1), then delete any existing DNS_TYPE_CNAME record for the node specified in pszNodeName, before adding the record. • If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found return a failure. Changed to: • If the pAddRecord is for an explicitly defined resource record type DNS_TYPE_CNAME (section 2.2.2.1.1), then delete any existing DNS_TYPE_CNAME record for the node specified in pszNodeName, before adding the record. • If pAddRecord is for adding a new record to a dnsNode that has or had a static resource record (with TimeStamp at 0), then the new record is added as a static record.<279> • If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found return a failure. <279> Section 3.1.4.5: New records added as static in dnsNodes that contain or contained a static record is supported in Windows Server 2008 and later.
2021/08/10	In Section 3.1.1.1.1 DNS Server Integer Properties, in DsTombstoneInterval added seconds to 100-nanosecond conversion. Changed from:

Errata Published*	Description
	DsTombstoneInterval: . . . Every day at 2:00 AM local time the DNS server MUST conduct a search of all zones stored in the directory server for nodes which have the dnsTombstoned attribute set to TRUE and an EntombedTime (section 2.2.2.2.4.23) value greater than DsTombstoneInterval seconds in the past. . . . Changed to: DsTombstoneInterval: . . . Every day at 2:00 AM local time the DNS server MUST conduct a search of all zones stored in the directory server for nodes which have the dnsTombstoned attribute set to TRUE and an EntombedTime (section 2.2.2.2.4.23) value greater than DsTombstoneInterval seconds in the past (convert seconds to 100-nanosecond intervals for comparison). . . . In Section 3.1.4.5 R_DnssrvUpdateRecord (Opnum 4), changed EntombedTime from seconds to 100-nanosecond intervals and removed redundant instructions. Changed from: If pszZoneName points to a primary zone, attempt to perform addition/deletion/update of the record. If the operation is successful, increment the zone serial number using serial number arithmetic [RFC1982]. If the last record at the node is being deleted and the zone is stored in the directory server, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and the node's dnsRecord (section 2.3.2.2) attribute to contain a DNS_RPC_RECORD_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number seconds since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC). If the zone is directory server-integrated and the update causes new or modified records to be committed to the directory, the new zone serial number MUST also be written to the Serial field of the dnsRecord attribute, as specified in2.3.2.2. If this operation deletes the last record from the node and the zone is directory server-integrated, the DNS server MUST set the node's DNS Node Tombstone State (section 3.1.1) to TRUE by setting the value of the dnsTombstoned attribute to TRUE and writing a DNS_RPC_RECORD_TS (section 2.2.2.2.4.23) in the dnsRecord attribute. Changed to: If pszZoneName points to a primary zone, attempt to perform addition/deletion/update of the record. If the operation is successful, increment the zone serial number using serial number arithmetic [RFC1982]. If the zone is directory server-integrated and the update causes new or modified records to be committed to the directory, the new zone serial number MUST also be written to the Serial field of the dnsRecord attribute (section 2.3.2.2). If the last record at the node is being deleted and the zone is stored in the directory server or is directory server-integrated, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and the node's dnsRecord attribute to contain a DNS_RPC_RECORD_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number of 100-nanosecond intervals since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

*Date format: YYYY/MM/DD

[MS-DPWSSN]: Devices Profile for Web Services (DPWS) Size Negotiation Extension

This topic lists the Errata found in [MS-DPWSSN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

[MS-DRSR]: Directory Replication Service (DRS) Remote Protocol

This topic lists the Errata found in the MS-DRSR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V42.0 – 2021/06/25.

Errata Published*	Description
2022/06/01	In Section 5.39 DRS_EXTENSIONS_INT: Modified the description of the Pid field in the DRS_EXTENSIONS_INT structure to clarify how the field is set, which is to the current client or server process. Also revised behavior note <42> to clarify that the Pid field is set to the current client or server process. Changed From: "Pid (4 bytes): A 32-bit, signed integer value that specifies the process identifier of the client. This is for informational and debugging purposes only. The assignment of this field is implementation specific. <42>" <42> This field contains the process ID of the client. Changed To: "Pid (4 bytes): A 32-bit, signed integer value that specifies a process identifier. The client sets the Pid field to the current client process. The server sets the Pid to the current server process. This is for informational and debugging purposes only. The assignment of this field is implementation-specific.<42>" <42> This field contains the process ID of the client or server, depending on which is current.

*Date format: YYYY/MM/DD

[MS-DTCO]: MSDTC Connection Manager: OleTx Transaction Protocol

This topic lists the Errata found in the MS-DTCO document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

December 1, 2017 - Download

[MS-DSCPM]: Desired State Configuration Pull Model Protocol

This topic lists the Errata found in the MS-DSCPM document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

December 1, 2017 - Download

September 12, 2018 - Download

[MS-DTYP]: Windows Data Types

This topic lists the Errata found in the MS-DTYP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

April 29, 2022 - Download

[MS-DVRD]: Device Registration Discovery Protocol

This topic lists the Errata found in [MS-DVRD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-DVRE]: Device Registration Enrollment Protocol

This topic lists the Errata found in the MS-DVRE document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-DVRJ]: Device Registration Join Protocol

This topic lists the Errata found in the MS-DVRJ document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-ECS]: Enterprise Client Synchronization Protocol

This topic lists the Errata found in the MS-ECS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

August 24, 2020 – Download

[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol

This topic lists the Errata found in the MS-EFSR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

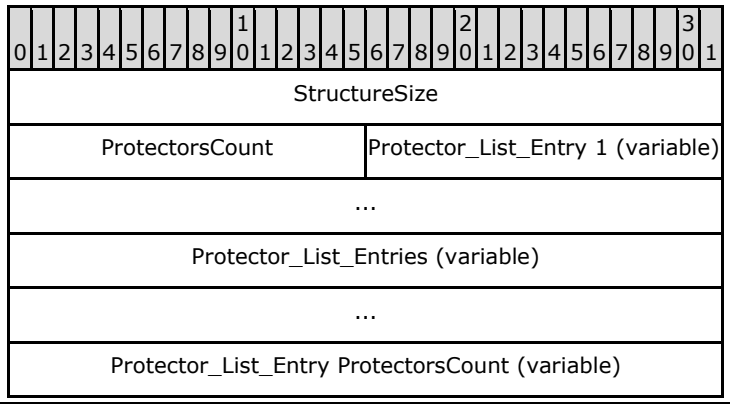
To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

October 6, 2021 - Download

April 29, 2022 - Download

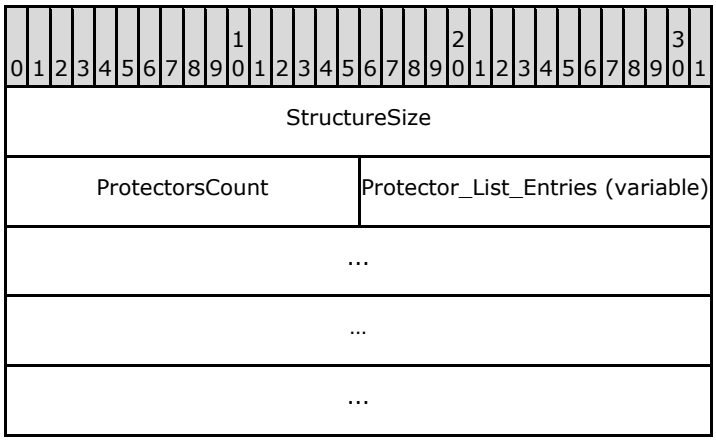
Errata below are for Protocol Document Version V30.0 – 2022/04/29.

Errata Published*	Description
2022/07/26	In section 3.1.4.2, EFSRPC Interface, added a product behavior note describing change after applying [MSFTE-CVE-2022-26925]: Changed from: The following table specifies the opnum associated with each RPC method in this protocol. An EFSRPC server SHOULD support all of the methods specified in this table.<37> Changed to: The following table specifies the opnum associated with each RPC method in this protocol. An EFSRPC server SHOULD support all of the methods specified in this table.<37><38> <38> Section 3.1.4.2: After installation of one of the updates listed in [MSFT-CVE-2022-26925], a client using a null session will receive RPC_S_ACCESS_DENIED when calling any of these methods using lsarpc.
2022/07/26	In section 2.2.2.2.1, Protector List Structure, removed two fields from structure diagram: Changed from: The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows. 

Errata Published*	Description
	...

Changed to:

The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.



*Date format: YYYY/MM/DD

[MS-EMF]: Enhanced Metafile Format

This topic lists the Errata found in the MS-EMF document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

April 7, 2021 - Download

April 29, 2022 - Download

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

This topic lists the Errata found in the MS-EMFPLUS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

March 4, 2020 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V19.0 – 2021/06/25.

Errata Published*	Description
2021/10/12	In Section 2.3.4.15, EmfPlusFillClosedCurve Record, amended descriptions of fill operations. Changed from: A "winding" fill operation fills areas according to the "even-odd parity" rule... An "alternate" fill operation fills areas according to the "non-zero" rule.... Changed to: An "alternate" fill operation fills areas according to the "even-odd parity" rule... A "winding" fill operation fills areas according to the "non-zero" rule....

*Date format: YYYY/MM/DD

[MS-EMFSPOOL]: Enhanced Metafile Spool Format

This topic lists the Errata found in the MS-EMFSPOOL document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-ERREF]: Windows Error Codes

This topic lists the Errata found in the MS-ERREF document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

April 7, 2021 - Download

[MS-EVEN]: EventLog Remoting Protocol

This topic lists the Errata found in the MS-EVEN document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V24.0 – 2021/06/25.

Errata Published*	Description
2021/07/27	In Section 2.1.2, Client: Changed from: The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<6> Changed to: The client MUST specify packet-level integrity authentication (0x5) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<6>.

*Date format: YYYY/MM/DD

[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

This topic lists the Errata found in the MS-EVEN6 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V24.0 – 2021/06/25.

Errata Published*	Description
2021/07/27	In Section 2.1.2, Client: Changed from: The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<5> Changed to: The client MUST specify packet-level integrity authentication (0x5) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<5>

*Date format: YYYY/MM/DD

[MS-FASP]: Firewall and Advanced Security Protocol

This topic lists the Errata found in the MS-FASP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

March 13, 2019 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version v31.0 – 2022/04/29.

Errata Published*	Description
2022/09/20	Section 3.1.4 Message Processing Events and Sequencing Description: Removed duplicate instances of 'unsigned' designator in subsections 3.1.4.59, 3.1.4.60, 3.1.4.62, 3.1.4.67, 3.1.4.68, 3.1.4.69, and 3.1.4.70. Section 3.1.6 Other Local Events Description: Added abstract interface definitions from subsections 3.1.6.1, 3.1.6.2, 3.1.6.3, 3.1.6.4, 3.1.6.5, 3.1.6.6, 3.1.6.7, and 3.1.6.8 to Section 6 Full IDL. Section 6 Full IDL Added policy store handle to the Full IDL. Added abstract interfaces to the Full IDL (definitions from sections 3.1.6.1, 3.1.6.2, 3.1.6.3, 3.1.6.4, 3.1.6.5, 3.1.6.6, 3.1.6.7, and 3.1.6.8). Replaced 'typedef struct _tag_FW_QUERY_CONDITIONS' in IDL with actual code instance.
2022/09/20	In Section 2.2.92: FW_QUERY_CONDITIONS Description: Updated definition of FW_QUERY_CONDITIONS struct. Changed from: typedef struct _tag_FW_QUERY_CONDITIONS {; unsigned LONG dwNumEntries; [size_is(dwNumEntries)] FW_QUERY_CONDITION* pAndedConditions; } FW_QUERY_CONDITIONS, *PFW_QUERY CONDITIONS; dwNumEntries: Specifies the number of query conditions that the structure contains. pAndedConditions: A pointer to an array of FW_QUERY_CONDITIONS elements, which are all logically AND'd together. The number of elements is given by dwNumEntries. Changed to: typedef struct_tag_FW_QUERY_CONDITIONS { DWORD dwNumEntries; [size_is(dwNumEntries)] FW_QUERY_CONDITION *AndedConditions; } FW_QUERY_CONDITIONS, *PFW_QUERY_CONDITIONS;

Errata Published*	Description
	dwNumEntries: Specifies the number of query conditions that the structure contains. AndedConditions: A pointer to an array of FW_QUERY_CONDITIONS elements, which are to be logically AND'd together by the server. Section 6 Appendix A Full IDL Changed from: Identical to the above. Changed to: Identical to the above.

[MS-FAX]: Fax Server and Client Remote Protocol

This topic lists the Errata found in the MS-FAX document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-FRS2]: Distributed File System Replication Protocol

This topic lists the Errata found in the MS-FRS2 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

April 7, 2021 - Download

[MS-FSA]: File System Algorithms

This topic lists the Errata found in the MS-FSA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

March 4, 2020 - Download

August 24, 2020 – Download

June 1, 2021 - Download

October 6, 2021 - Download

Errata below are for Protocol Document Version 36.0 – 2022/04/29.

Errata Published*	Description

2022/08/09	In section 2.1.5.15.11, FileRenameInformation, revised renaming processing.
	
	Changed from:
	
	▪ If *RemoveSourceLink* is TRUE:
	  ▪ If **Open.File.FileType** is DirectoryFile
	  ▪ *FilterMatch* = FILE_NOTIFY_CHANGE_DIR_NAME
	▪ Else
	  ▪ *FilterMatch* = FILE_NOTIFY_CHANGE_FILE_NAME
	▪ EndIf
	▪ If *MoveToNewDir* is TRUE or *AddTargetLink* is FALSE or *RemoveTargetLink* and *ExactCaseMatch* are TRUE: *Action* = FILE_ACTION_REMOVED
	▪ Else
	  ▪ *Action* = FILE_ACTION_REMOVED_OLD_NAME
	▪ EndIf
	
	Changed to:

Errata Published*	Description
	▪ If *RemoveSourceLink* is TRUE: ▪ If **Open.File.FileType** is DirectoryFile ▪ *FilterMatch* = FILE_NOTIFY_CHANGE_DIR_NAME ▪ Else ▪ *FilterMatch* = FILE_NOTIFY_CHANGE_FILE_NAME ▪ EndIf ▪ If *MoveToNewDir* is TRUE or *AddTargetLink* is FALSE or *RemoveTargetLink* and *ExactCaseMatch* are TRUE: *Action* = FILE_ACTION_REMOVED ▪ Else ▪ *Action* = FILE_ACTION_RENAMED_OLD_NAME ▪ EndIf
2022/07/26	Added revisions to section 2.1.5.2, Server Requests an Open of a Named Pipe. Please see the diff file.
2022/06/01	Added new section, 2.1.5.2, Server Requests an Open of a Named Pipe. Please see the diff file.
2022/06/01	In section 2.1.5.15.11, FileRenameInformation, added information about how NTFS prevents a race condition during renaming. Changed from: If Open.File contains open files as specified in section 2.1.4.2, the operation MUST be failed with STATUS_ACCESS_DENIED. Changed to: If Open.File contains open files as specified in section 2.1.4.2, the operation MUST be failed with STATUS_ACCESS_DENIED.<174> <174> On Windows NTFS, NTFS checks for open files beneath the directory being renamed (performs section 2.1.4.2), it records the count of open files. If there is a lease to break, NTFS requests the break and then goes back to the start of performing 2.1.5.15.11. NTFS waits for the lease break acknowledgment and restarts the rename operation. When NTFS performs section 2.1.4.2 again, it again records how many open files there are beneath the directory and compares that to the previous count. If the current count is greater than or equal to the previous count, NTFS fails the rename and prevents a possible race condition.
2022/05/27	In section 2.1.5.10.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated list of applicable updates. Changed from: <127> Section 2.1.5.10.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is handled following the process in this section on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023]. Changed to: <127> Section 2.1.5.10.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is handled following the process in this section on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].
2022/05/18	The following sections were changed. Please see the diff document for the details. In Section 2.1.1.3, Per File, updated a product behavior about how registry entries affect the handling of LastAccessTime: Changed from: <17> Section 2.1.1.3: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry key: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A nonzero value means LastAccessTime updates are disabled. A value of zero means they are enabled. Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<17> Section 2.1.1.3: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry values (respectively): HKLM\System\CurrentControlSet\Control\FileSystem\RefsDisableLastAccessUpdate, and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A value of 1 means LastAccessTime updates are disabled. Any other value (or undefined) means they are enabled.

In Windows 10 v1803 operating system and subsequent, NTFS has two registry values controlling LastAccessTime updates: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate and HKLM\System\CurrentControlSet\Control\FileSystem\ NtfsLastAccessUpdatePolicyVolumeSizeThreshold. The NtfsDisableLastAccessUpdate value is now treated as a bitfield as follows:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000001</td><td>Disable LastAccessTime updates.</td></tr>
<tr><td>0x00000002</td><td>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:
On client systems, LastAccessTime updates are enabled if any of the following conditions are true:
• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.
• The size of the boot volume is <= NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.
• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is <= 128GB.
On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.
At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</td></tr>
<tr><td>0x80000000</td><td>Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.</td></tr>
</table>
If the value of NtfsDisableLastAccessUpdate is controlled by group policy, then only flag 0x00000001 is recognized.

In Section 2.1.1.4, Per Link, updated a product behavior about how registry entries affect the handling of LastAccessTime:

Changed from:

<31> Section 2.1.1.4: In Windows Vista and subsequent LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry key:
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A nonzero value means LastAccessTime updates are disabled. A value of zero means they are enabled.

Changed to:

<31> Section 2.1.1.4: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is updated only when the file is closed. This behavior is controlled by the following registry values (respectively): HKLM\System\CurrentControlSet\Control\FileSystem\RefsDisableLastAccessUpdate, and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A value of 1 means LastAccessTime updates are disabled. Any other value (or undefined) means they are enabled.

In Windows 10 v1803 and subsequent, NTFS has two registry values controlling LastAccessTime updates: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate and HKLM\System\CurrentControlSet\Control\FileSystem\ NtfsLastAccessUpdatePolicyVolumeSizeThreshold. The NtfsDisableLastAccessUpdate value is now treated as a bitfield as follows:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000001</td><td>Disable LastAccessTime updates.</td></tr>
<tr><td>0x00000002</td><td>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:
On client systems, LastAccessTime updates are enabled if any of the following conditions are true:
• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.
• The size of the boot volume is less than or equal to NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.
• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is <= 128GB.
On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.
At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</td></tr>
<tr><td>0x80000000</td><td>Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.</td></tr>
</table>
If the value of NtfsDisableLastAccessUpdate is controlled by group policy, then only flag 0x00000001 is recognized.
</td></tr>
</table>

Errata Published*	Description
2022/05/02	In Section 2.1.5.9.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated processing rules for system versions. Changed from: The server provides:<127> <127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). Changed to: The server provides:<127> <127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is handled following the process in this section on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023].

[MS-FSCC]: File System Control Codes

This topic lists the Errata found in the MS-FSCC document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V52.0 – 2022/04/29.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/08/09</td><td>In section 2.7.1, FILE_NOTIFY_INFORMATION, revised descriptions of the values in the Action field.

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>FILE_ACTION_ADDED
0x00000001</td><td>The file was added to the directory.</td></tr>
<tr><td>FILE_ACTION_REMOVED
0x00000002</td><td>The file was removed from the directory. When a file is renamed to a different directory the client will receive this notification along with FILE_ACTION_MODIFIED.</td></tr>
<tr><td>FILE_ACTION_MODIFIED
0x00000003</td><td>The file was modified. This can be a change to the data or attributes of the file. When a file is renamed to a different directory the client will receive this notification along with FILE_ACTION_REMOVED.</td></tr>
</table>

Changed to:</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>FILE_ACTION_ADDED
0x00000001</td><td>The file was renamed, and FileName contains the new name. This notification is only sent when the rename operation changes the directory the file resides in. The client will also receive a FILE_ACTION_REMOVED notification. This notification will not be received if the file is renamed within a directory.</td></tr>
<tr><td>FILE_ACTION_REMOVED
0x00000002</td><td>The file was renamed, and FileName contains the old name. This notification is only sent when the rename operation changes the directory the file resides in. The client will also receive a FILE_ACTION_ADDED notification. This notification will not be received if the file is renamed within a directory.</td></tr>
<tr><td>FILE_ACTION_MODIFIED
0x00000003</td><td>The file was modified. This can be a change to the data or attributes of the file.</td></tr>
</table>
</td></tr>
<tr><td>2022/05/27</td><td>In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, updated list of applicable updates.

Changed from:
<76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023].

Changed to:

<76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].</td></tr>
<tr><td>2022/05/02</td><td>In Section 2.1.5.9.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated processing rules for system versions.

Changed from:

The server provides:<127>

<127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher).

Changed to:

The server provides:<127>

<127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is handled following the process in this section on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023].</td></tr>
</table>

[MS-FSRVP]: File Server Remote VSS Protocol

This topic lists the Errata found in the MS-FSRVP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

[MS-FSVCA]: File Set Version Comparison Algorithms

This topic lists the Errata found in the MS-FSVCA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-GPPREF]: Group Policy: Preferences Extension Data Structure

This topic lists the Errata found in [MS-GPPREF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

September 12, 2018 - Download

[MS-GPSB]: Group Policy: Security Protocol Extension

This topic lists the Errata found in [MS-GPSB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

September 12, 2018 - Download

[MS-GPOL]: Group Policy: Core Protocol

This topic lists the Errata found in [MS-GPOL] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-GPWL]: Group Policy: Wireless/Wired Protocol Extension

This topic lists the Errata found in [MS-GPWL] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-GSSA]: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension

This topic lists the Errata found in the MS-GSSA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-HGSA]: Host Guardian Service: Attestation Protocol

This topic lists the Errata found in the MS-HGSA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

[MS-HTTPE]: Hypertext Transfer Protocol (HTTP) Extensions

This topic lists the Errata found in [MS-HTTPE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-HVRS]: Hyper-V Remote Storage Profile

This topic lists the Errata found in [MS-HVRS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 20, 2017 - Download

[MS-ICPR]: ICertPassage Remote Protocol

This topic lists the Errata found in the MS-ICPR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-IKEE]: Internet Key Exchange Protocol Extensions

This topic lists the Errata found in the MS-IKEE document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

September 15, 2017 - Download

April 7, 2021 - Download

[MS-IPAMM2]: IP Address Management (IPAM) Management Protocol Version 2

This topic lists the Errata found in [MS-IPAMM2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

[MS-IPHTTPS]: IP over HTTPS (IP-HTTPS) Tunneling Protocol

This topic lists the Errata found in the MS-IPHTTPS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-IRP]: Internet Information Services (IIS) Inetinfo Remote Protocol

This topic lists the Errata found in [MS-IRP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-KILE]: Kerberos Protocol Extensions

This topic lists the Errata found in [MS-KILE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V39.0 – 2022/04/29.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/11/08</td><td>In section 2.2.7 Supported Encryption Types Bit Flags: Added encryption type AES256-CTS-HMAC-SHA1-96-SK to position 20+6 designated by J.

Changed from:
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
0 0 0 0 0 0 0 0 0 0 0 0 I H G F 0 0 0 0 0 0 0 0 0 0 E D C B A

<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>A</td><td>DES-CBC-CRC</td></tr>
<tr><td>. . .</td><td></td></tr>
<tr><td>I</td><td>Resource-SID-compression-disabled<12></td></tr>
</table>

Changed to:
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
0 0 0 0 0 0 0 0 0 0 0 0 I H G F 0 0 0 0 0 0 0 0 0 0 J E D C B A</td></tr>
</table>

Errata Published*	Description
	<table><tr><th>Value</th><th>Description</th></tr><tr><td>A</td><td>DES-CBC-CRC</td></tr><tr><td>. . .</td><td></td></tr><tr><td>I</td><td>Resource-SID-compression-disabled<12></td></tr><tr><td>J</td><td>AES256-CTS-HMAC-SHA1-96-SK</td></tr></table> In section 3.1.5.2 Encryption Types: Replaced SHOULD with MUST support the AES encryption types. Removed RC4-HMAC-EXP [24]. Changed from: KILE SHOULD support the Advanced Encryption Standard (AES) encryption types: ● AES256-CTS-HMAC-SHA1-96 [18] ([RFC3962] section 7) ● AES128-CTS-HMAC-SHA1-96 [17] ([RFC3962] section 7)and SHOULD<24> support the following encryption types, which are listed in order of relative strength: ● RC4-HMAC [23] [RFC4757] ● RC4-HMAC-EXP [24] [RFC4757] ● DES-CBC-MD5 [3] [RFC3961] ● DES-CBC-CRC [1] [RFC3961] <24> Section 3.1.5.2: In Windows… RC4-HMAC and RC4-HMAC-EXP are supported in Windows. … Changed to: KILE MUST support the Advanced Encryption Standard (AES) encryption types: ● AES256-CTS-HMAC-SHA1-96 [18] ([RFC3962] section 7) ● AES128-CTS-HMAC-SHA1-96 [17] ([RFC3962] section 7)and SHOULD<24> support the following encryption types, which are listed in order of relative strength: ● RC4-HMAC [23] [RFC4757] ● DES-CBC-MD5 [3] [RFC3961] ● DES-CBC-CRC [1] [RFC3961] <24> Section 3.1.5.2: In Windows… RC4-HMAC is supported in Windows. … In section 5.1.5 DES Downgrade Protection: Removed RC4 support.

Errata Published*	Description
	Changed from: Since KILE has the ability to configure a principal as supporting only DES, and unarmored AS exchanges are vulnerable to downgrade attacks, the KDC can protect against DES downgrade attacks by not supporting DES for principals that are not DES-only. Since all KILE KDCs support at least RC4, RC4 can always be used for KDCs and their hosts. Additionally, all KILE hosts support at least RC4, so RC4 can always be used for service tickets to hosts. Thus,DES usage is required only for trusts to non-KILE realms and services using non-KILE servers that do not support RC4 or AES. Changed to: Since KILE has the ability to configure a principal as supporting only DES, and unarmored AS exchanges are vulnerable to downgrade attacks, the KDC can protect against DES downgrade attacks by not supporting DES for principals that are not DES-only. DES usage is required only for trusts to non-KILE realms and services using non-KILE servers that do not support RC4 or AES.

*Date format: YYYY/MM/DD

[MS-KPP]: Key Provisioning Protocol

This topic lists the Errata found in the MS-KPP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-KPS]: Key Protection Service Protocol

This topic lists the Errata found in the MS-KPP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

September 15, 2017 - Download

[MS-LCID]: Windows Language Code Identifier (LCID) Reference

This topic lists the Errata found in [MS-LCID] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 13, 2019 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V15.0 – 2021/06/25.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2022/05/02</td><td>In Section 2.2, LCID Structure, added the following language IDs to the table:

0x2000 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

0x2400 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

0x2800 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.
0x2C00 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

In Section 2.2.1, Locale Names without LCIDs, updated the table:

Changed from:

<table>
<tr><th>Name</th><th>Value</th><th>Conditions</th></tr>
<tr><td>LOCALE_CUSTOM_USER_DEFAULT<15></td><td>0x0C00</td><td>When an LCID without a permanent LCID assignment is also the current user locale, the protocol will respond with LOCALE_CUSTOM_USER_DEFAULT for that locale. This assignment persists until the user changes the locale. Because the meaning changes over time, applications are discouraged from persisting this data. Though this value will likely refer to the same locale for the lifetime of the current process, that is not guaranteed. This assignment is a 1-to-</td></tr>
</table>
</td></tr>
</table>

Errata Published *	Description

		1 relationship between this LCID and the user's current default locale name.
Transient LCIDs<16>	0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400, 0x4800, 0x4C00	Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 8 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the machine, or other machines, and, as such, is unsuitable for use in protocols or persisted data. This assignment is a temporary 1-to-1 relationship between an LCID and a particular locale name and will round trip until that relationship changes.

Changed to:

Name	Value	Conditions
LOCALE_CUSTOM_USER_DEFAULT<15>	0x0C00	When an LCID without a permanent LCID assignment is also the current user locale, the protocol will respond with LOCALE_CUSTOM_USER_DEFAULT for that locale. This assignment persists until the user changes the locale. Because the meaning changes over time, applications are discouraged from persisting this data. Though this value will likely refer to the same locale for the lifetime of the current process, that is not guaranteed. This assignment is a 1-to-1 relationship between this LCID and the user's current default locale name.
Transient LCIDs<16>	0x2000, 0x2400, 0x2800, 0x2C00,0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400, 0x4800, 0x4C00	Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 12 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the machine, or other machines, and, as such, is unsuitable for use in protocols or persisted data. This assignment is a temporary 1-to-1 relationship

Errata Published *	Description		
			between an LCID and a particular locale name and will round trip until that relationship changes.

*Date format: YYYY/MM/DD

[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol

This topic lists the Errata found in [MS-LSAD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

March 16, 2018 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version 45.0 2021/06/25.

Errata Published*	Description
2022/09/20	In Section 2.2.1.4, AEAD-AES-256-CBC-HMAC-SHA512 Constants Description: Updated AEAD-AES-256-CBC-HMAC-SHA512 constants to ensure that the value details allow an implementation to be successfully created. Changed from: **Constant Name** / **Value** versionbyte / 0x01 versionbyte_length / 1 SAM_AES_256_ALG / "AEAD-AES-256-CBC-HMAC-SHA512" SAM_AES256_ENC_KEY_STRING / "Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16" SAM_AES256_MAC_KEY_STRING / "Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16" SAM_AES256_ENC_KEY_STRING_LENGTH / sizeof(SAM_AES256_ENC_KEY_STRING) SAM_AES256_MAC_KEY_STRING_LENGTH / sizeof(SAM_AES256_MAC_KEY_STRING) Changed to: **Constant Name** / **Meaning** Versionbyte / Version identifier

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>0x01</td><td></td></tr>
<tr><td>versionbyte_length
1</td><td>Version identifier length</td></tr>
<tr><td>SAM_AES_256_ALG
"AEAD-AES-256-CBC-HMAC-SHA512"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING
"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING
"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH
sizeof(SAM_AES256_ENC_KEY_STRING)
(61)</td><td>The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH
sizeof(SAM_AES256_MAC_KEY_STRING)
(54)</td><td>The length of SAM_AES256_MAC_KEY_STRING, including the null terminator</td></tr>
</table>

In Section 5.1.5 AES Cipher Usage
Description: Clarified the usage of enc_key and mac_key when encrypting the data.

Changed from:
"...
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)"

Changed to:
"...
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)
Note that enc_key is truncated to 32-bytes and the entire 64-byte mac_key is used."
</td></tr>
<tr><td>2022/01/11</td><td>The following sections in the table below are updated or new.
Please see the PDF diff document for details.
<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td>1.3 Overview</td><td>Updated</td></tr>
<tr><td>1.6 Applicability Statement</td><td>Updated</td></tr>
<tr><td>2.2 Common Data Types</td><td>Updated</td></tr>
<tr><td>2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants</td><td>Created new section</td></tr>
<tr><td>2.2.1.5 LSA Trust Record Flags</td><td>Created new section</td></tr>
<tr><td>2.2.2.6 LSAPR_REVISION_INFO_V1</td><td>Created new</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description	
		section
	2.2.2.7 LSAPR_REVISION_INFO	Created new section
	2.2.7.2 TRUSTED_INFORMATION_CLASS	Updated
	2.2.7.3 LSAPR_TRUSTED_DOMAIN_INFO	Updated
	2.2.7.21 LSA_FOREST_TRUST_RECORD	Updated
	2.2.7.22 LSA_FOREST_TRUST_RECORD_TYPE	Updated
	2.2.7.30 LSAPR_TRUSTED_DOMAIN_FULL_INFORMATION_INTERNAL_AES	Created new section
	2.2.7.31 LSA_FOREST_TRUST_SCANNER_INFO	Created new section
	2.2.7.32 LSA_FOREST_TRUST_RECORD2	Created new section
	2.2.7.33 LSA_FOREST_TRUST_INFORMATION2	Created new section
	3.1.1.5 Trusted Domain Object Data Model	Updated
	3.1.4 Message Processing Events and Sequencing Rules	Updated
	3.1.4.4.9 LsarOpenPolicy3 (Opnum 130)	Created new section
	3.1.4.7.15 LsarQueryForestTrustInformation (Opnum 73)	Updated
	3.1.4.7.16 LsarSetForestTrustInformation (Opnum 74)	Updated
	3.1.4.7.17 LsarCreateTrustedDomainEx3 (Opnum 129)	Created new section
	3.1.4.7.18 LsarQueryForestTrustInformation2 (Opnum 132)	Created new section
	3.1.4.7.19 LsarSetForestTrustInformation2 (Opnum 133)	Created new section
	5.1.5 AES Cipher Usage	Created new section
	5.2 Index of Security Parameters	Updated
	6 Appendix A: Full IDL	Updated

[MS-LSAT]: Local Security Authority (Translation Methods) Remote Protocol

This topic lists the Errata found in [MS-LSAT] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

June 1, 2017 - Download

September 15, 2017 - Download

April 7, 2021 - Download

[MS-MDE]: Mobile Device Enrollment Protocol

This topic lists the Errata found in [MS-MDE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

September 15, 2017 - Download

[MS-MDE2]: Mobile Device Enrollment Protocol Version 2

This topic lists the Errata found in [MS-MDE2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

June 1, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version 12.0 - 2022/04/29.

Errata Published*	Description
2022/10/03	<14> Section 3.1.4.1.3.1 DiscoveryRequest, updated product note with RequestVersion v5.0 support from Windows 11 (version 2) to Windows 11 (version 1) 2022 10C patch and later. Changed From: RequestVersion value 5.0 is supported only in the Windows 11, version 22H2 operating system and later. Changed To: RequestVersion value 5.0 is supported only in Windows 11 (version 1), 2022 10C patch and later. In the following sections updated the product notes with EnrollmentVersion v5.0 support from Windows 11 (version 2) to Windows 11 (version 1) 2022 10C patch and later. <15> Section 3.1.4.1.3.2 DiscoveryResponse <16> Section 3.3.4.1.1.2 GetPoliciesResponse <17> Section 3.3.4.1.1.2 GetPoliciesResponse <20> Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication <23> Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication <26> Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication Changed From: EnrollmentVersion value 5.0 is supported only in Windows 11 v22H2 and later, see section

Errata Published*	Description
	3.1.4.1.3.2. Changed To: EnrollmentVersion value 5.0 is supported only in Windows 11 (version 1), 2022 10C patch and later, see section 3.1.4.1.3.2.

[MS-MDM]: Mobile Device Management Protocol

This topic lists the Errata found in [MS-MDM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

December 1, 2017 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version 14.0 - 2022/04/29

Errata Published*	Description
2022/06/14	In section 2.1 Transport: Added Note 9 to indicate client behavior when the ForceAadToken in the DMClient configuration service provider is set by the server. Changed from: . . . Note 8: If the server has set EntDMID in the DMClient configuration service provider, the client adds client-request-id to the header and sets it to the value of EntDMID.<9> See [MSDOCS-DMClient-CSP] for more information. Changed to: . . . Note 8: If the server has set EntDMID in the DMClient configuration service provider, the client adds client-request-id to the header and sets it to the value of EntDMID.<9> See [MSDOCS-DMClient-CSP] for more information. Note 9: If the server has set ForceAadToken in the DMClient configuration service provider, and the device is joined to an Azure Active Domain (AAD), the client adds a custom header that contains the AAD token. The header is in the following format. DeviceToken: CI6MTQxmCF5xgu6yYcmV9ng6vhQfaJYw… See [MSDOCS-DMClient-CSP] for more information.<10> Appendix B: <10> Section 2.1: Not available in Windows 10 v19H2 and earlier.
2022/05/02	3.2.5.1 Windows Azure Virtual Desktop for Multi-users' User Setting Configuration, added a product note that the added support for user sessions multi-session Edition only in WVD was backported.

Errata Published*	Description
	Changed from: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously. To allow configuration of user settings, the MDM server must support "multi-user AVD" mode… Changed to: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<15> To allow configuration of user settings, the MDM server must support "multi-user AVD" mode… <15> Section 3.2.5.1: Servicing May 2022, support for user sessions on Windows 11, version 22H2 operating system (version 2) multi-session Edition only in Windows Virtual Desktop was backported to Windows 11 (version 1).

[MS-MICE]: Miracast over infrastructure Connection Establishment Protocol

This topic lists the Errata found in [MS-MICE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-MSSOD]: Media Streaming Server Protocols Overview

This topic lists the Errata found in [MS-MSSOD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

December 1, 2017 - Download

[MS-MWBE]: Microsoft Web Browser Federated Sign-On Protocol Extensions

This topic lists the Errata found in [MS-MWBE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the following ERRATA archive:

June 30, 2015 - Download

[MS-MWBF]: Microsoft Web Browser Federated Sign-On Protocol

This topic lists the Errata found in [MS-MWBF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

September 12, 2018 - Download

[MS-NBTE]: NetBIOS over TCP (NetBT) Extensions

This topic lists the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 29, 2022 – Download

[MS-NCNBI]: Network Controller Northbound Interface Specification

This topic lists the Errata found in the MS-NCNBI document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.
Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 16, 2018 - Download

September 12, 2018 - Download

April 7, 2021 - Download

April 29, 2022 - Download

[MS-NCT]: Network Cost Transfer Protocol

This topic lists the Errata found in the MS-NCT document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-NFPB]: Near Field Proximity Bidirectional Services Protocol

This topic lists the Errata found in [MS-NFPB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-NFPS]: Near Field Proximity Sharing Protocol

This topic lists the Errata found in [MS-NFPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-NKPU]: Network Key Protector Unlock Protocol

This topic lists the Errata found in [MS-NKPU] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

December 1, 2017 - Download

[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol

This topic lists the Errata found in [MS-NLMP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 23, 2019 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V35.0 – 2022/04/29.

Errata Published*	Description
2022/07/26	In section 2.2.1.2 CHALLENGE_MESSAGE: Added statement that the server MUST return the NTLMSSP_NEGOTIATE_SIGN if set by the client. Changed from: NegotiateFlags (4 bytes): A NEGOTIATE structure that contains a set of flags, as defined by section 2.2.2.5. The server sets flags to indicate options it supports or, if there has been a NEGOTIATE_MESSAGE (section 2.2.1.1), the choices it has made from the options offered by the client. Changed to: NegotiateFlags (4 bytes): A NEGOTIATE structure that contains a set of flags, as defined by section 2.2.2.5. The server sets flags to indicate options it supports or, if there has been a NEGOTIATE_MESSAGE (section 2.2.1.1), the choices it has made from the options offered by the client. If the client has set the NTLMSSP_NEGOTIATE_SIGN in the NEGOTIATE_MESSAGE the Server MUST return it.

Date format: YYYY/MM/DD

[MS-NMFMB]: .NET Message Framing MSMQ Binding Protocol

This topic lists the Errata found in [MS-NMFMB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

December 1, 2017 - Download

[MS-NNS]: .NET NegotiateStream Protocol

This topic lists the Errata found in [MS-NNS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

Errata below are for Protocol Document Version V7.0 – 2017/12/01.

Errata Published*	Description
2019/02/19	In Section 2.2.2, Data Message, the maximum size of the PayloadSize field has been changed from '0x0000FC00' to '0x0000FC30', to accommodate for both the application data size and the size increase that occurs when this protocol signs or encrypts the data to be transferred. Changed from: PayloadSize (4 bytes): The unsigned size, in bytes, of the Payload field. The maximum value for this field is 0x0000FC00 (that is, 63K, or 64,512). Changed to: PayloadSize (4 bytes): The unsigned size, in bytes, of the Payload field. The maximum value for this field is 0x0000FC30 (64,560).

*Date format: YYYY/MM/DD

[MS-NRBF]: .NET Remoting: Binary Format Data Structure

This topic lists the Errata found in [MS-NRBF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V12.0 – 2019/03/13.

Errata Published*	Description
2019/10/28	In Section 3.0, Structure Examples, in the logical Request message for dotNET_Framework 1.1, changed the BinaryMethodCall value from: BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x21) MessageEnum: 00000014 Changed to: BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x15) MessageEnum: 00000014

*Date format: YYYY/MM/DD

[MS-NRPC]: Netlogon Remote Protocol

This topic lists the Errata found in [MS-NRPC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 23, 2019 - Download

August 24, 2020 – Download

April 7, 2021 - Download

June 24, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V40.0 2022/04/29.

Errata Published*	Description
2022/11/08	In section 3.1.1 Abstract Data Model: SealSecureChannel removed duplicate and adjusted to the encryption setting MUST be TRUE. Removed statement with note <69> about storing and retrieving the SealSecureChannel variable. Changed from: TrustPasswordVersion: ... SealSecureChannel: ... StrongKeySupport: ... The Netlogon client and server variables are as follows: LocatedDCsCache: ... 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<69> persistently store and retrieve the SealSecureChannel variable. VulnerableChannelAllowList: A setting expressed in Security Descriptor Definition Language (SDDL) ([MS-DTYP] section 2.5.1) of Netlogon client allowed to not use secure bindings, see section 3.1.4.6.<70>

Errata Published*	Description
	Changed to: TrustPasswordVersion: ... StrongKeySupport: ... The Netlogon client and server variables are as follows: LocatedDCsCache: ... SealSecureChannel: A Boolean setting that indicates whether the RPC message has to be encrypted or just integrity-protected ([C706] section 13.2.5). This setting MUST be TRUE. VulnerableChannelAllowList: A setting expressed in Security Descriptor Definition Language (SDDL) ([MS-DTYP] section 2.5.1) of Netlogon client allowed to not use secure bindings, see section 3.1.4.6.<69> In section 3.1.4.6 Calling Methods Requiring Session-Key Establishment: Step 1: Replaced if…TRUE... with: Clients MUST request the Privacy authentication level. Step 4: Added RPC Integrity to the MUST deny request list. Updated product note. Changed from: The client and server follow this sequence of steps.<75> 1. The client SHOULD<76> bind to the RPC server using TCP/IP. The client and server MUST utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] 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 from the RPC runtime. If the SealSecureChannel setting is FALSE, then the authentication level requested is Integrity. 2. … 3. … 4. If secure bind is not used, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<77> <75> Section 3.1.4.6: Windows XP and later clients will request secure RPC. Windows Server 2008 R2 operating system and later will enforce that clients are using RPC Integrity and Confidentiality to secure the connection. For more information, see [MSFT-CVE-2020-1472]. Changed to: The client and server follow this sequence of steps.<74> 1. The client SHOULD<75> bind to the RPC server using TCP/IP. The client and server MUST utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] section 2.2.1.1.7) for privacy/integrity of the RPC messages. Clients MUST request the Privacy authentication level. 2. … 3. …

Errata Published*	Description
	4. If secure bind is not used or the client is using RPC Integrity instead of RPC Privacy, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<76> <74> Section 3.1.4.6: Windows XP and later clients will request secure RPC. Windows Server 2008 and later will enforce that clients are using RPC Confidentiality to secure the connection. For more information, see [MSFT-CVE-2020-1472] and [MSFT-CVE-2022-38023]. In section 3.4.1 Abstract Data Model: RequireSignOrSeal: Added that this setting MUST be TRUE. Changed from: RequireSignOrSeal: Indicates whether the client SHOULD<87> continue session-key negotiation when the server did not specify support for Secure RPC as described in the negotiable option Y of section 3.1.4.2. Changed to: RequireSignOrSeal: Indicates whether the client SHOULD<87> continue session-key negotiation when the server did not specify support for Secure RPC as described in the negotiable option Y of section 3.1.4.2. This setting MUST be TRUE. In section 3.4.3 Initialization: Changed RequireSignOrSeal from SHOULD to MUST be initialized to TRUE. Changed from: RequireSignOrSeal SHOULD<92> be initialized to TRUE. Changed to: RequireSignOrSeal MUST<92> be initialized to TRUE. In section 3.5.1 Abstract Data Model: SignSecureChannel: Added This setting is deprecated, as SealSecureChannel MUST be TRUE. Changed from: SignSecureChannel: A Boolean variable that determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates. Changed to: SignSecureChannel: A Boolean variable that determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates. This setting is deprecated, as SealSecureChannel MUST be TRUE. In Section 3.5.3 Initialization: RejectMD5Clients, SealSecureChannel, and SignSecureChannel set to TRUE.

Errata Published*	Description
	Changed from: RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to FALSE. SealSecureChannel SHOULD be TRUE. SignSecureChannel SHOULD be initialized in an implementation-specific way and set to 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). Changed to: RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to TRUE. SealSecureChannel MUST be TRUE. SignSecureChannel SHOULD be initialized in an implementation-specific way and set to 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). This setting is deprecated, as SealSecureChannel MUST be true.
2022/09/20	In section 1.3.1 Pass-Through Authentication: Added little endian usage statement. Changed from: … The secure channel is achieved by encrypting the communication traffic with a session key computed using a secret key (called a server's machine account password) shared by the server and the DC. Changed to: … The secure channel is achieved by encrypting the communication traffic with a session key computed using a secret key (called a server's machine account password) shared by the server and the DC. Unless otherwise specified, MS-NRPC uses little endian for byte ordering before encryption. In section 2.2.1.3.7 NL_TRUST_PASSWORD: Added product note about little endian usage for big endian users. Changed from: . . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire. Changed to: . . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire.<24> <24> Section 2.2.1.3.7: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed. In section 3.4.5.2.5 Calling NetrServerPasswordSet2: Added product note about little endian usage for big endian users. Changed from: 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 established as the encryption key. Changed to: Encrypt <98> the ClearNewPassword parameter using the negotiated encryption algorithm

Errata Published*	Description
	(determined by bits C, O, or W, respectively, in the NegotiateFlags member of the ServerSessionInfo table entry for PrimaryName) and the session key established as the encryption key. <98> Section 3.4.5.2.5: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed. In section 3.5.4.4.5 NetrServerPasswordSet2 (Opnum 30): Added product note about little endian usage for big endian users. Changed from: ClearNewPassword: A pointer to an NL_TRUST_PASSWORD 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). Changed to: ClearNewPassword: A pointer to an NL_TRUST_PASSWORD structure, as specified in section 2.2.1.3.7, that contains the new password encrypted<178> as specified in Calling NetrServerPasswordSet2 (section 3.4.5.2.5). <178> Section 3.5.4.4.5: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed.

[MS-NSPI]: Name Service Provider Interface (NSPI) Protocol

This topic lists the Errata found in [MS-NSPI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-OAPX]: OAuth 2.0 Protocol Extensions

This topic lists the Errata found in [MS-OAPX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

[MS-OAPXBC]: OAuth 2.0 Protocol Extensions for Broker Clients

This topic lists the Errata found in [MS-OAPXBC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

September 26, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

October 6, 2021 - Download

[MS-OCSPA]: Microsoft OCSP Administration Protocol

This topic lists the Errata found in [MS-OCSPA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions

This topic lists the Errata found in [MS-OIDCE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

October 6, 2021 - Download

[MS-OLEDS]: Object Linking and Embedding (OLE) Data Structures

This topic lists the Errata found in [MS-OLEDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

December 1, 2017 - Download

September 12, 2018 - Download

[MS-OLEPS]: Object Linking and Embedding (OLE) Property Set Data Structures

This topic lists the Errata found in [MC-OLEPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-OTPCE]: One-Time Password Certificate Enrollment Protocol

This topic lists the Errata found in [MS-OTPCE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

RSS
Atom

Errata are subject to the same terms as the Open Specifications documentation referenced.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-PAC]: Privilege Attribute Certificate Data Structure

This topic lists the Errata found in [MS-PAC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

November 23, 2020 - Download

April 29, 2022 - Download

[MS-PAR]: Print System Asynchronous Remote Protocol

This topic lists the Errata found in [MS-PAR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

April 7, 2021 - Download

[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)

This topic lists the Errata found in [MS-PEAP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-PKAP]: Public Key Authentication Protocol

This topic lists the Errata found in the MS-PKAP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

This topic lists the Errata found in [MS-PKCA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 6, 2021 - Download

Errata below are for Protocol Document Version V15.0 – 2021/10/06.

Errata Published*	Description
2022/05/10	Section 3.1.5.2.1.5 Mapping Strength: added section. The KDC SHOULD<22> map a certificate to a user using one of the following mappings. These methods of mapping a certificate to a user are classified as strong or weak based on whether they depend on a name as a secure identifier. The following mappings are considered weak: • SAN UPNName • SAN DNSName • altSecurityIdentities Issuer Name and Subject Name • altSecurityIdentities Subject Name • altSecurityIdentities 822 field The following mappings are considered strong: • SID (section 3.1.5.2.1.6) • Key Trust (section 3.1.5.2.1.4) • altSecurityIdentities Issuer and Serial Number • altSecurityIdentities Subject Key Identifier • altSecurityIdentities SHA1 Hash of Public Key If a KDC maps a certificate to a user using one of the above weak mappings, it SHOULD<23> continue to search for more mappings until it encounters a strong mapping. If it does not find such a mapping, it MAY fail the authentication request with KDC_ERR_CERTIFICATE_MISMATCH.

Errata Published*	Description
	<22> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later. <23> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later. Section 3.1.5.2.1.6 SID: added section. If a KDC has exhausted all other mapping types for a certificate and found a weak mapping without finding a strong mapping, it SHOULD<24> check if the certificate contains a security identifier (SID). If it does and the SID matches the user the certificate weakly mapped to, the certificate is to be considered strongly mapped. If the SID does not match, the authentication MUST fail with KDC_ERR_CERTIFICATE_MISMATCH. If the certificate does not contain a SID, the KDC MAY fail the authentication request as no strong mapping is available. For more details on the objectSID in an issued certificate see [MS-WCCE] and section 2.2.2.7.7.4. <24> Section 3.1.5.2.1.6 Certificate SID mapping is applicable to Windows Server 2008 R2 and later.

*Date format: YYYY/MM/DD

[MS-PSRDP]: PowerShell Remote Debugging Protocol

This topic lists the Errata found in [MS-PSRDP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-PSRP]: PowerShell Remoting Protocol

This topic lists the Errata found in [MS-PSRP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-RA]: Remote Assistance Protocol

This topic lists the Errata found in [MS-RA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-RAI]: Remote Assistance Initiation Protocol

This topic lists the Errata found in [MS-RAI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

April 7, 2021 - Download

[MS-RDPADRV]: Remote Desktop Protocol Audio Level and Drive Letter Persistence Virtual Channel Extension

This topic lists the Errata found in [MS-RDPADRV] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting

This topic lists the Errata found in [MS-RDPBCGR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V55.0 – 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/01/04</td><td>In section 2.2.1.3.2, Client Core Data (TS_UD_CS_CORE), added the client version number for RDP 10.10:

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00080001</td><td>RDP 4.0 clients</td></tr>
<tr><td>0x00080004</td><td>RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 clients</td></tr>
<tr><td>0x00080005</td><td>RDP 10.0 clients</td></tr>
<tr><td>0x00080006</td><td>RDP 10.1 clients</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

0x00080007	RDP 10.2 clients
0x00080008	RDP 10.3 clients
0x00080009	RDP 10.4 clients
0x0008000A	RDP 10.5 clients
0x0008000B	RDP 10.6 clients
0x0008000C	RDP 10.7 clients
0x0008000D	RDP 10.8 clients
0x0008000E	RDP 10.9 clients

Changed to:

Value	Meaning
0x00080001	RDP 4.0 clients
0x00080004	RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 clients
0x00080005	RDP 10.0 clients
0x00080006	RDP 10.1 clients
0x00080007	RDP 10.2 clients
0x00080008	RDP 10.3 clients
0x00080009	RDP 10.4 clients
0x0008000A	RDP 10.5 clients
0x0008000B	RDP 10.6 clients
0x0008000C	RDP 10.7 clients
0x0008000D	RDP 10.8 clients
0x0008000E	RDP 10.9 clients
0x0008000F	RDP 10.10 clients

In section 2.2.1.4.2, Server Core Data (TS_UD_SC_CORE), added the server version number for RDP 10.10:

Changed from:

Value	Meaning
0x00080001	RDP 4.0 servers
0x00080004	RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers

Errata Published*	Description
	0x00080005 | RDP 10.0 servers 0x00080006 | RDP 10.1 servers 0x00080007 | RDP 10.2 servers 0x00080008 | RDP 10.3 servers 0x00080009 | RDP 10.4 servers 0x0008000A | RDP 10.5 servers 0x0008000B | RDP 10.6 servers 0x0008000C | RDP 10.7 servers 0x0008000D | RDP 10.8 servers 0x0008000E | RDP 10.9 servers Changed to: Value | Meaning 0x00080001 | RDP 4.0 servers 0x00080004 | RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers 0x00080005 | RDP 10.0 servers 0x00080006 | RDP 10.1 servers 0x00080007 | RDP 10.2 servers 0x00080008 | RDP 10.3 servers 0x00080009 | RDP 10.4 servers 0x0008000A | RDP 10.5 servers 0x0008000B | RDP 10.6 servers 0x0008000C | RDP 10.7 servers 0x0008000D | RDP 10.8 servers 0x0008000E | RDP 10.9 servers 0x0008000F | RDP 10.10 servers

*Date format: YYYY/MM/DD

[MS-RDPEA]: Remote Desktop Protocol: Audio Output Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-RDPEAR]: Remote Desktop Protocol Authentication Redirection Virtual Channel

This topic lists the Errata found in [MS-RDPEAR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 15, 2017 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V7.0 – 2021/06/25.

Errata Published*	Description

2021/09/07	In Section 2.2 Message Syntax, changed data types in TSRemoteGuardInnerPacket.
	
	Changed from:
	
	`TSRemoteGuardInnerPacket ::= SEQUENCE {`
	`  version  [0] TSRemoteGuardVersion DEFAULT tsremoteguardv1,`
	`  packageName  [1] OCTETSTRINGNOCOPY,`
	`  buffer  [2] OCTETSTRINGNOCOPY,`
	`  extension  [3] ANYNOCOPY OPTIONAL,  -- future extension point`
	`  ...`
	`}`
	
	Changed to:
	
	`TSRemoteGuardInnerPacket ::= SEQUENCE {`
	`  version  [0] TSRemoteGuardVersion DEFAULT tsremoteguardv1,`
	`  packageName  [1] OCTET STRING,`
	`  buffer  [2] OCTET STRING,`
	`  extension  [3] ANY OPTIONAL,  -- X.680 open type for future extension point`
	`  ...`
	`}`

*Date format: YYYY/MM/DD

[MS-RDPECLIP]: Remote Desktop Protocol: Clipboard Virtual Channel Extension

This topic lists the Errata found in [MS-RDPECLIP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V15.0 – 2021/06/25.

Errata Published*	Description
2022/09/03	In Section 4.4.3.1, Requesting the Size of a File, revised example: Changed from: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 01 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 .... 00000020 00 00 00 00 00 00 00 00 .... Changed to: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 01 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 .... In Section 4.4.3.2, Requesting the Contents of a File, revised example: Changed from: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 02 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 ....

Errata Published*	Description
	00000020 00 00 00 00 00 00 00 00 .... Changed to: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 02 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 ....

*Date format: YYYY/MM/DD

[MS-RDPECAM]: Remote Desktop Protocol: Video Capture Virtual Channel Extension

This topic lists the Errata found in [MS-RDPECAM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-RDPEDISP]: Remote Desktop Protocol: Display Update Virtual Channel Extension

This topic lists the Errata found in the MS-RDPEDISP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-RDPEDYC]: Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEDYC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

[MS-RDPEFS]: Remote Desktop Protocol: File System Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEFS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

[MS-RDPEGDI]: Remote Desktop Protocol: Graphics Device Interface (GDI) Acceleration Extensions

This topic lists the Errata found in [MS-RDPEGDI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-RDPEGFX]: Remote Desktop Protocol: Graphics Pipeline Extension

This topic lists the Errata found in [MS-RDPEGFX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

[MS-RDPEGT]: Remote Desktop Protocol Geometry Tracking Virtual Channel Protocol Extension

This topic lists the Errata found in [MS-RDPEGFT] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-RDPEI]: Remote Desktop Protocol: Input Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPELE]: Remote Desktop Protocol: Licensing Extension

This topic lists the Errata found in [MS-RDPELE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

[MS-RDPEMC]: Remote Desktop Protocol: Multiparty Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEMC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPEMT]: Remote Desktop Protocol: Multitransport Extension

This topic lists the Errata found in [MS-RDPEMT] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - Download

April 7, 2021 - Download

[MS-RDPEPC]: Remote Desktop Protocol: Print Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEPC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-RDPEPNP]: Remote Desktop Protocol: Plug and Play Devices Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEPNP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPERP]: Remote Desktop Protocol: Remote Programs Virtual Channel Extension

This topic lists the Errata found in [MS-RDPERP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

April 7, 2021 - Download

[MS-RDPESC]: Remote Desktop Protocol: Smart Card Virtual Channel Extension

This topic lists the Errata found in [MS-RDPESC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

[MS-RDPESP]: Remote Desktop Protocol: Serial and Parallel Port Virtual Channel Extension

This topic lists the Errata found in [MS-RDPESP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPEUDP]: Remote Desktop Protocol: UDP Transport Extension

This topic lists the Errata found in [MS-RDPEUDP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

September 23, 2019 - Download

August 24, 2020 – Download

[MS-RDPEUDP2]: Remote Desktop Protocol: UDP Transport Extension Version 2

This topic lists the Errata found in [MS-RDPEUDP2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 13, 2019 - Download

September 23, 2019 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V5.0 – 2021/06/25.

Errata Published*	Description
2021/08/17	In Section 3.1.5.2, DelayAckInfo Payload, changed case of a field name: Changed from: maxDelayedAcks Changed to: MaxDelayedAcks In Section 3.1.5.7, Acknowledgement Vector Payload, revised a field name: Changed from: AckVecSize Changed to: codedAckVecSize
2021/08/17	In Section 2.2.1.2.2, OverheadSize Payload, revised the value of OVERHEADSIZE. Changed from: OVERHEADSIZE (0x10) Changed to: OVERHEADSIZE (0x040)

Errata Published*	Description
	In Section 2.2.1.2.3, DelayAckInfo Payload, revised the value of DELAYACKINFO. Changed from: DELAYACKINFO (0x20) Changed to: DELAYACKINFO (0x100) In Section 2.2.1.2.4, AckOfAcks Payload, revised the value of AOA. Changed from: AOA (0x08) Changed to: AOA (0x010) In Section 2.2.1.2.5, DataHeader Payload, revised the value of DATA. Changed from: DATA (0x02) Changed to: DATA (0x004) In Section 2.2.1.2.6, Acknowledgement Vector Payload, revised the value of ACKVEC. Changed from: ACKVEC (0x04) Changed to: ACKVEC (0x008) In Section 2.2.1.2.7, DataBody Payload, revised the value of DATA. Changed from: DATA (0x02) Changed to:

Errata Published*	Description
	DATA (0x004)

*Date format: YYYY/MM/DD

[MS-RDPEV]: Remote Desktop Protocol: Video Redirection Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEV] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPEVOR]: Remote Desktop Protocol: Video Optimized Remoting Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEVOR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

[MS-RDPEXPS]: Remote Desktop Protocol: XML Paper Specification (XPS) Print Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEXPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-RDPRFX]: Remote Desktop Protocol: RemoteFX Codec Extension

This topic lists the Errata found in [MS-RDPRFX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-RMPR]: Rights Management Services (RMS): Client-to-Server Protocol

This topic lists the Errata found in [MS-RMPR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-RMSOD]: Rights Management Services Protocols Overview

This topic lists the Errata found in [MS-RMSOD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

[MS-RNAS]: Vendor-Specific RADIUS Attributes for Network Policy and Access Server (NPAS) Data Structure

This topic lists the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V5.0 – 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/02/08</td><td>In section 2.2.1.11 MS-Azure-Policy-ID, added new section

Changed from:

Changed to:

The MS-Azure-Policy-ID is a VSA, as specified in section 2.2.1. It is used by the Radius Server to send an identifier which is used by Azure Point to Site VPN Server to match an authenticated RADIUS user Policy configured on the Azure side. This Policy is used to select IP/ Routing configuration (assigned IP address) for the user. The fields of MS-Azure-Policy-ID MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x41.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the octet string in the Attribute-Specific Value plus 2.

Attribute-Specific Value: An octet string containing the Policy ID configured on the Azure Point to Site VPN Server.

In section 3.1.5.2 Microsoft VSA Support of RADIUS Messages, added MS-Azure-Policy-ID VSA to table.

Changed from:

<table>
<tr><th>Microsoft vendor-specific attribute</th><th>Request</th><th>Accept</th><th>Reject</th><th>Challenge</th><th>Accounting-Request</th></tr>
<tr><td>. . .</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>MS-RDG-Device-Redirection</td><td>0</td><td>0-1</td><td>0</td><td>0</td><td>0</td></tr>
</table>

Changed to:</td></tr>
</table>

Errata Published*	Description
	<table><tr><th>Microsoft vendor-specific attribute</th><th>Request</th><th>Accept</th><th>Reject</th><th>Challenge</th><th>Accounting-Request</th></tr><tr><td>. . .</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>MS-RDG-Device-Redirection</td><td>0</td><td>0-1</td><td>0</td><td>0</td><td>0</td></tr><tr><td>MS-Azure-Policy-ID</td><td>0</td><td>0-1</td><td>0</td><td>0</td><td>0</td></tr></table> In section 3.3.5.2.3 MS-Azure-Policy-ID, added new section Changed from: Changed to: This attribute is consumed only by the Microsoft Azure Point to Site VPN Server. When a Microsoft Azure Point to Site VPN Server receives this attribute in an Access-Accept message, it applies the IP/ Routing configuration set against Policy-id received for that user. A NAS that is not a Microsoft Azure Point to Site VPN Server ignores this attribute. For more details about this attribute, see section 2.2.1.11.

*Date format: YYYY/MM/DD

[MS-RPCE]: Remote Procedure Call Protocol Extensions

This topic lists the Errata found in the MS-RPCE document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

September 15, 2017 - Download

April 7, 2021 - Download

[MS-RPCH]: Remote Procedure Call over HTTP Protocol

This topic lists the Errata found in [MS-RPCH] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-RPRN]: Print System Remote Protocol

This topic lists the Errata found in [MS-RPRN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

December 1, 2017 - Download

August 24, 2020 – Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

[MS-RRASM]: Routing and Remote Access Server (RRAS) Management Protocol

This topic lists the Errata found in [MS-RRASM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

[MS-RRP]: Windows Remote Registry Protocol

This topic lists the Errata found in the MS-RRP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

March 4, 2020 - Download

April 7, 2021 - Download

[MS-RSMC]: Remote Session Monitoring and Control Protocol

This topic lists the Errata found in [MS-RSMC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

[MS-RSVD]: Remote Shared Virtual Disk Protocol

This topic lists the Errata found in [MS-RSVD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 26, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

April 29, 2022 - Download

[MS-SAMR]: Security Account Manager (SAM) Remote Protocol (Client-to-Server)

This topic lists the Errata found in [MS-SAMR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V45.0- 2022/04/29.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/09/20</td><td>In Section 2.2.1.18, AEAD-AES-256-CBC-HMAC-SHA512 Constants
Description: Updated AEAD-AES-256-CBC-HMAC-SHA512 constants to ensure that the value details allow an implementation to be successfully created.

Changed from:
<table>
<tr><th>Constant Name</th><th>Value</th></tr>
<tr><td>versionbyte</td><td>0x01</td></tr>
<tr><td>versionbyte_length</td><td>1</td></tr>
<tr><td>SAM_AES_256_ALG</td><td>"AEAD-AES-256-CBC-HMAC-SHA512"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING</td><td>"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING</td><td>"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_ENC_KEY_STRING)</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_MAC_KEY_STRING)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Changed to:
<table>
<tr><th>Constant/value</th><th>Description</th></tr>
<tr><td>Versionbyte
0x01</td><td>Version identifier.</td></tr>
<tr><td>versionbyte_length
1</td><td>Version identifier length.</td></tr>
<tr><td>SAM_AES_256_ALG
“AEAD-AES-256-CBC-HMAC-SHA512”</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING
"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING
"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH
sizeof(SAM_AES256_ENC_KEY_STRING)
(61)</td><td>The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH
sizeof(SAM_AES256_MAC_KEY_STRING)
(54)</td><td>The length of SAM_AES256_MAC_KEY_STRING, including the null terminator</td></tr>
</table>
In Section 3.2.2.4, AES Cipher Usage
Description: Specified the format of secret plaintext for SamrUnicodeChangePasswordUser4 and SamrSetInformationUser2 when creating the content encryption key (CEK); and clarified the usage of enc_key and mac_key when encrypting the data.
Changed from:
• For the SamrUnicodeChangePasswordUser4 method (section 3.1.5.10.4), the shared secret is the plaintext old password and the CEK is generated as specified in section 3.2.2.5.
Changed to:
• For the SamrUnicodeChangePasswordUser4 method (section 3.1.5.10.4), the shared secret is the plaintext old password and the CEK is generated as specified in section 3.2.2.5.
• For SamrUnicodeChangePasswordUser4 and SamrSetInformationUser2, the secret plaintext MUST be in the format specified in section 2.2.6.32.
Changed from:
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)
Changed to:
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)
Note that enc_key is truncated to 32-bytes and the entire 64-byte mac_key is used.
In Section 3.2.2.5 Deriving an Encryption Key from a Plaintext Password
Description: Clarified how a 16-byte encryption key MUST be derived.
Changed from:
The client MUST derive the CEK in the following manner:
CEK :: = (PBKDF2(NT HASH of “OldPassword”, Salt, Iteration Count, 512))
Changed to:
The client MUST derive the CEK in the following manner:
A 16-byte encryption key is derived using the PBKDF2 algorithm with HMAC SHA-512, the NT-hash of the users existing password, a random 16-byte Salt, and an Iteration Count.
</td></tr>
</table>

Errata Published*	Description
	The Iteration Count MUST be between 5000 and 1,000,000 inclusive. CEK :: = (PBKDF2(NT HASH of "OldPassword", Salt, Iteration Count, 16))

*Date format: YYYY/MM/DD

[MS-SAMS]: Security Account Manager (SAM) Remote Protocol (Server-to-Server)

This topic lists the Errata found in the MS-KPP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-SCMR]: Service Control Manager Remote Protocol

This topic lists the Errata found in [MS-SCMR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

September 23, 2019 - Download

April 29, 2022 – Download

[MS-SHLLINK]: Shell Link (.LNK) Binary File Format

This topic lists the Errata found in [MS-SHLLINK] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-SFMWA]: Server and File Management Web APIs

This topic lists the Errata found in [MS-SFMWA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 20, 2017 - Download

[MS-SFU]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol

This topic lists the Errata found in the MS-SFU document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 4, 2020 - Download

November 23, 2020 - Download

Errata below are for Protocol Document Version V21.0 – 2021/06/25.

Errata Published*	Description
2021/09/21	In Section 3.2.5.2.3 Using ServicesAllowedToReceiveForwardedTicketsFrom, removed the UserAccountControl check and added a behavior note to document the addition of the NonForwardableDelegation flag with references to the Kerberos Security Feature Bypass Vulnerability. Changed from: If the service ticket in the additional-tickets field is not set to forwardable,<22> and the USER_NOT_DELEGATED bit is set in the UserAccountControl field in the KERB_VALIDATION_INFO structure ([MS-PAC] section 2.5), then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1). Changed to: If the service ticket in the additional-tickets field is not set to forwardable,<22> then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1).<23> <23> Section 3.2.5.2.3: The Kerberos Security Feature Bypass Vulnerability March 12,2021 [MSFT-CVE-2020-16996] update adds support for the NonForwardableDelegation registry value to (0) enable Enforcement of protection on Active Directory domain controller servers. Active Directory domain controllers will be in Enforcement mode unless the enforcement mode registry key is set to (1) disabled. This update applies to Windows Server 2012 and later. For additional information that includes Windows Server 2008 SP2 operating system and Windows Server 2008 R2 SP1 operating system see [MSFT-RBCD-ProtectedUserChanges].

*Date format: YYYY/MM/DD

[MS-SMB]: Server Message Block (SMB) Protocol

This topic lists the Errata found in [MS-SMB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

[MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3

This topic lists the Errata found in [MS-SMB2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

June 1, 2021 - Download

October 6, 2021 - Download

Errata below are for Protocol Document Version V66.0 – 2022/04/29.

Errata Published*	Description
2022/09/20	In Section 3.1.4.4, Compressing the Message, made the description generic because different implementations can make different criteria to determein when to compress on not to compress the data: Changed from: • Otherwise if RemainingUncompressedDataSize is greater than zero and (size of the uncompressed SMB2 message / RemainingUncompressedDataSize) is greater than 2, CompressedMessage MUST be appended with newly constructed SMB2_COMPRESSION_CHAINED_PAYLOAD_HEADER. CompressionAlgorithm MUST be set to NONE. Length MUST be set to RemainingUncompressedDataSize. CompressedMessage MUST be appended with the uncompressed data. RemainingUncompressedDataSize MUST be decremented by the size of data before compression. TotalCompressedDataSize MUST be incremented by the size of compressed data. Changed to: • Otherwise, if an implementation decides that the cost of remaining operations that might require copying the data is worth the encryption savings, then CompressedMessage MUST be appended with newly constructed SMB2_COMPRESSION_CHAINED_PAYLOAD_HEADER. CompressionAlgorithm MUST be set to NONE. Length MUST be set to RemainingUncompressedDataSize. CompressedMessage MUST be appended with the uncompressed data. RemainingUncompressedDataSize MUST be decremented by the size of data before compression. TotalCompressedDataSize MUST be incremented by the size of compressed data.
2022/09/03	In section 3.2.4.3, Application Requests Opening a File, added product behavior notes to clarify how leases are handled: Changed from:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>If an entry is not found, a new File entry MUST be created and added to the GlobalFileTable and a File.LeaseKey,<131> as specified in section 3.2.1.5, MUST be assigned to the entry. File.OpenTable MUST be initialized to an empty table and File.LeaseState MUST be initialized to SMB2_LEASE_NONE.

...
Otherwise, if Connection.SupportsFileLeasing is TRUE, the client SHOULD set RequestedOplockLevel field to SMB2_OPLOCK_LEVEL_LEASE.

Changed to:

If an entry is not found, a new File entry MUST be created and added to the GlobalFileTable and a File.LeaseKey,<131> as specified in section 3.2.1.5, MUST be assigned to the entry.<132> File.OpenTable MUST be initialized to an empty table and File.LeaseState MUST be initialized to SMB2_LEASE_NONE.

If an entry is found, the client MUST include a lease context with the existing lease key, lease state, and epoch.<133>

...

● Otherwise, if Connection.SupportsFileLeasing is TRUE, the client SHOULD<135> set RequestedOplockLevel field to SMB2_OPLOCK_LEVEL_LEASE.

<132> Section 3.2.4.3: On Windows 7 operating system and Windows Server 2008 R2, a 128-bit ClientLeaseId is generated by an arithmetic combination of LeaseKey and ClientGuid, which is passed to the object store at open/create time. On Windows 8 operating system and later and Windows Server 2012 operating system and later, the LeaseKey in the request is used as the ClientLeaseId.
<133> Section 3.2.4.3: On Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the Lease.ClientLeaseId and Lease.ParentLeaseKey are passed to the object store in the form of TargetOplockKey and ParentOplockKey. A new or existing lease is thereby associated with the resulting open.
To acquire or promote the lease as dictated by the SMB2_CREATE_REQUEST_LEASE_V2 Create Context, a subsequent object store call is invoked as described in. [MS-FSA] section 2.1.5.18 Server Requests an Oplock. The Open parameter passed is the Open result from the above operation, and the Type parameter is LEVEL_GRANULAR to indicate a Lease request. The RequestedOplockLevel field is constructed to include zero or more bits as follows.
<table>
<tr><th>Object Store RequestedOplockLevel bit to be set</th><th>SMB2 Lease.LeaseState bit requested</th></tr>
<tr><td>READ_CACHING</td><td>SMB2_LEASE_READ_CACHING</td></tr>
<tr><td>WRITE_CACHING</td><td>SMB2_LEASE_WRITE_CACHING</td></tr>
<tr><td>HANDLE_CACHING</td><td>SMB2_LEASE_HANDLE_CACHING</td></tr>
</table>

The Status code returned indicates whether the requested lease was granted.

<135> Section 3.2.4.3: Microsoft Windows lease-aware clients always include SMB2_OPLOCK_LEVEL_LEASE if the open can potentially cause a lease break.</td></tr>
<tr><td>2022/07/26</td><td>In Section 3.2.4.3 Application Requests Opening a File, updated what file elements client uses when it accesses same path across multiple opens.</td></tr>
</table>

Errata Published*	Description
	Changed From: If the client accesses a file through multiple paths, such as using different server names or share names or parent directory names, it will create multiple File elements, and therefore multiple File.LeaseKeys for the same remote file. This loses the performance benefits of sharing cache state across all Opens of the same file and can cause additional lease breaks to be generated, as actions by a client through one path will affect caching by that client through other paths. However, the impact is a matter of performance; cache correctness is preserved. Changed To: If the client accesses a file through multiple paths, such as using different server names or share names or parent directory names, it will create multiple File elements, and therefore multiple File.LeaseKeys for the same remote file. This loses the performance benefits of sharing cache state across all Opens of the same file and can cause additional lease breaks to be generated, as actions by a client through one path will affect caching by that client through other paths. However, the impact is a matter of performance; cache correctness is preserved. If the client accesses same path across multiple opens, the client will use same File element and therefore same File.LeaseKey is used. In Section 3.2.4.3.8 Requesting a Lease on a File or a Directory, updated setting of LeaseKey field for SMB2_CREATE_REQUEST_LEASE_V2 create context Changed From: . LeaseKey obtained from File.LeaseKey of the file or directory being opened. Changed To: . LeaseKey is set to File.LeaseKey obtained from section 3.2.4.3.
2022/07/12	In Section 3.2.4.3 Application Requests Opening a File, updated what file elements client uses when it accesses same path across multiple opens. Changed From: If the client accesses a file through multiple paths, such as using different server names or share names or parent directory names, it will create multiple File elements, and therefore multiple File.LeaseKeys for the same remote file. This loses the performance benefits of sharing cache state across all Opens of the same file and can cause additional lease breaks to be generated, as actions by a client through one path will affect caching by that client through other paths. However, the impact is a matter of performance; cache correctness is preserved. Changed To: If the client accesses a file through multiple paths, such as using different server names or share names or parent directory names, it will create multiple File elements, and therefore multiple File.LeaseKeys for the same remote file. This loses the performance benefits of sharing cache state across all Opens of the same file and can cause additional lease breaks to be generated, as actions by a client through one path will affect caching by that client through other paths. However, the impact is a matter of performance; cache correctness is preserved. If the client accesses same path across multiple opens, the client will use same File element and therefore same File.LeaseKey is used. In Section 3.2.4.3.8 Requesting a Lease on a File or a Directory, updated setting of LeaseKey field for SMB2_CREATE_REQUEST_LEASE_V2 create context Changed From: . LeaseKey obtained from File.LeaseKey of the file or directory being opened.

Errata Published*	Description
	Changed To: . LeaseKey is set to File.LeaseKey obtained from section 3.2.4.3.
2022/06/28	In Section 2.2.41 SMB2 TRANSFORM_HEADER, updated the definition of signature field. Changed from: Signature (16 bytes): The 16-byte signature of the encrypted message generated by using Session.EncryptionKey. Changed to: Signature (16 bytes): The 16-byte signature of the message generated using negotiated encryption algorithm. In Section 2.2.43.1 SMB2_RDMA_CRYPTO_TRANSFORM, updated the definition of signature field. Changed from: Signature (variable): The signature of the encrypted/signed data generated using Session.EncryptionKey. The length of this field MUST be less than or equal to 16 bytes. Changed to: Signature (variable): The signature of the data generated using negotiated encryption/signing algorithm. The length of this field MUST be less than or equal to 16 bytes.
2022/06/28	In section 3.2.5.15, Receiving an SMB2 Query_Directory response, added information about a case where STATUS_BUFFER_OVERFLOW is returned and the buffer content length is zero. Changed from: If the Status field of the SMB2 header of the response indicates success, the client MUST copy the received information in the SMB2 QUERY_DIRECTORY Response following the SMB2 header that is described by the OutputBufferOffset and OutputBufferLength into the buffer that is provided by the calling application. The client MUST return success and the OutputBufferLength to the application. Changed to: If the Status field of the SMB2 header of the response indicates success, the client MUST copy the received information in the SMB2 QUERY_DIRECTORY Response following the SMB2 header that is described by the OutputBufferOffset and OutputBufferLength into the buffer that is provided by the calling application. The client MUST return success and the OutputBufferLength to the application. There can be cases where STATUS_BUFFER_OVERFLOW is returned and the OutputBufferSize is set to zero. See [MSDOCS-ABEConcepts] for an example of such a case where output entries are filtered when the requester does not have the required permissions. [MS-FSA] section 2.1.5.6.3 describes the algorithm.
2022/06/01	In Section 3.3.5.9.12 Handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context, updated setting Epoch field in the case of handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 with SMB2_CREATE_REQUEST_LEASE_V2 create context.

Errata Published*	Description
	Changed From: . If Lease.LeaseState includes SMB2_LEASE_WRITE_CACHING, the server MUST set Lease.Epoch to the Epoch field in the Create Context request. Otherwise, the server MUST set Lease.Epoch to the Epoch field in the Create Context request incremented by 1. Epoch MUST be set to Lease.Epoch. Changed To: . Epoch SHOULD<329> be set to Lease.Epoch. <329> When an open, with Open.IsPersistent set to TRUE, is being reconnected due to server failover, Windows Server 2012 operating system and later perform the following: . If Lease.LeaseState includes SMB2_LEASE_WRITE_CACHING, Epoch and Lease.Epoch are set to Epoch field in the Create Context request. . If Lease.LeaseState does not include SMB2_LEASE_WRITE_CACHING, Epoch and Lease.Epoch are set to Epoch field in the Create Context request incremented by 1.
2022/06/01	In Section 3.2.4.4 Re-establishing a Durable Open, updated setting Epoch field in the case of re-establishing a durable open with SMB2_CREATE_REQUEST_LEASE_V2 create context. Changed From: . If Connection.Dialect is not "2.0.2", and the original open was performed by using a lease as described in section 3.2.4.3.8, as indicated by Open.OplockLevel set to SMB2_OPLOCK_LEVEL_LEASE, it MUST also implement the following: . The client MUST re-request the lease as described in section 3.2.4.3.8, and the LeaseState field MUST be set to File.LeaseState of the file being opened. Changed To: . If Connection.Dialect is not "2.0.2", and the original open was performed by using a lease as specified in section 3.2.4.3.8, as indicated by Open.OplockLevel set to SMB2_OPLOCK_LEVEL_LEASE, the client MUST re-request the lease as specified in section 3.2.4.3.8 with the exception of the following values: . The LeaseState field MUST be set to File.LeaseState of the file being opened. . If Connection.Dialect belongs to the SMB 3.x dialect family, the Epoch field MUST be set to File.LeaseEpoch of the file being opened.
2022/06/01	In Section 3.3.4.7, Object Store Indicates an Oplock Break, updated the text to address the Open issues and setting of lease state. Changed from: If a Lease entry is found, the server MUST perform the following: If Lease.LeaseOpens is empty, the server MUST complete the lease break call from the underlying object store with "NONE" as the new lease state, set Lease.LeaseState to "NONE", and take no further action. Otherwise, for the specified Open, the server MUST select the connection as specified in section 3.3.4.1.6. If no connection is available, for each Open in Lease.LeaseOpens, the server MUST close the Open as specified in section 3.3.4.17 for the following cases: ● Open.IsDurable, Open.IsResilient, and Open.IsPersistent are all FALSE. ● Lease.BreakToLeaseState does not contain SMB2_LEASE_HANDLE_CACHING and

Errata Published*	Description
	Open.IsDurable is TRUE. … Otherwise, the server MUST set the Flags field of the message to SMB2_NOTIFY_BREAK_LEASE_FLAG_ACK_REQUIRED, indicating to the client that lease acknowledgment is required. The LeaseKey field MUST be set to Lease.LeaseKey. The server MUST set Open.OplockState to "Breaking" for all Opens in Lease.LeaseOpens. The server MUST set the CurrentLeaseState field of the message to Lease.LeaseState, set Lease.Breaking to TRUE, set Lease.BreakToLeaseState to the new lease state indicated by the object store, and set Lease.LeaseBreakTimeout to the current time plus an implementation-specific<227> default value in milliseconds. Changed to: If a Lease entry is found, the server MUST perform the following: If Lease.LeaseOpens is empty, the server MUST complete the lease break call from the underlying object store with "NONE" as the new lease state, set Lease.LeaseState to "NONE", and take no further action. If no connection is available among all Opens in Lease.LeaseOpens, the server MUST close every Open as specified in section 3.3.4.17 in one of the following cases: ● Open.IsDurable, Open.IsResilient, and Open.IsPersistent are all FALSE. ● The new lease state indicated by object store does not contain SMB2_LEASE_HANDLE_CACHING and Open.IsDurable is TRUE. … Otherwise, the server MUST set the Flags field of the message to SMB2_NOTIFY_BREAK_LEASE_FLAG_ACK_REQUIRED, indicating to the client that lease acknowledgment is required. The LeaseKey field MUST be set to Lease.LeaseKey. The server MUST set Open.OplockState to "Breaking" for all Opens in Lease.LeaseOpens. The server MUST set the CurrentLeaseState field of the message to Lease.LeaseState, set Lease.Breaking to TRUE, set Lease.BreakToLeaseState and NewLeaseState field to the new lease state indicated by the object store, and set Lease.LeaseBreakTimeout to the current time plus an implementation-specific<227> default value in milliseconds.
2022/05/27	In section 3.3.5.15, Receiving an SMB2 IOCTL Request, updated the list of applicable updates. Changed from: Processing of FSCTL_SET_INTEGRITY_INFORMATION_EX is handled as described in [MS-FSA] and [MS-FSCC] when the system is updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], and [MSKB-5014023]. Changed to: Processing of FSCTL_SET_INTEGRITY_INFORMATION_EX is handled as described in [MS-FSA] and [MS-FSCC] when the system is updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].
2022/05/18	In Section 3.3.5.22.2, Processing a Lease Acknowledgment, updated the text to remove the symbols: Changed from: If LeaseState is not <= Lease.BreakToLeaseState, the server MUST fail the request with STATUS_REQUEST_NOT_ACCEPTED. Changed to: If LeaseState is not a subset of Lease.BreakToLeaseState, the server MUST fail the request with STATUS_REQUEST_NOT_ACCEPTED.
2022/05/02	In Section 3.3.5.15, Receiving an SMB2 IOCTL Request, updated processing rules for system versions. Changed from: The server SHOULD<355> fail the request with STATUS_NOT_SUPPORTED when an FSCTL is not allowed on the server, and SHOULD<356> fail the request with

Errata Published*	Description
	STATUS_INVALID_DEVICE_REQUEST when the FSCTL is allowed, but is not supported on the file system on which the file or directory handle specified by the FSCTL exists, as specified in [MS-FSCC] section 2.2. Changed to: The server SHOULD<355> fail the request with STATUS_NOT_SUPPORTED when an FSCTL is not allowed on the server, and SHOULD<356> fail the request with STATUS_INVALID_DEVICE_REQUEST when the Processing of FSCTL_SET_INTEGRITY_INFORMATION_EX is handled as described in [MS-FSA] and [MS-FSCC] when the system is updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], and [MSKB-5014023]. FSCTL is allowed, but is not supported on the file system on which the file or directory handle specified by the FSCTL exists, as specified in [MS-FSCC] section 2.2.

[MS-SMBD]: SMB2 Remote Direct Memory Access (RDMA) Transport Protocol

This topic lists the Errata found in [MS-SMBD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

April 7, 2021 - Download

[MS-SPNG]: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension

This topic lists the Errata found in [MS-SPNG] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

April 29, 2022 – Download

[MS-SQOS]: Storage Quality of Service Protocol

This topic lists the Errata found in [MS-SQOS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)

This topic lists the Errata found in [MS-SSTP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

RSS
Atom

Errata are subject to the same terms as the Open Specifications documentation referenced.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V20.0 – 2021/06/25.

Errata Published*	Description
2022/10/24	In section 3.1.5.2 SSTP Packet Processing: Added MTU and MUR rules and settings that enable packets larger than 1586 bytes. Changed from: SSTP packet processing for common messages is covered separately for the client state machine and server state machine, in sections 3.2.5.3 and 3.3.5.2. Changed to: Common packet processing functionality is as follows: 1. The default maximum transmission unit (MTU) is set to 1400 bytes. 2. The maximum receive unit (MRU) exchanged for SSTP is 4091 bytes, which is 4095 – sizeof(SSTP_HEADER). 3. The default MTU can be increased using the registry values, but it is still capped at the MRU of the tunnel type. 4. The default MRU for the PPP adapter is set to 1614 bytes. 5. The default MRU can be increased by setting the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\MRU By default, packets of any size can be sent or received through the tunnel, as Windows stack will IP fragment the packets. To enable large SSTP payloads, both MTU (on the sender) and MRU (on the receiver) need to be set to larger values. SSTP packet processing for common messages is covered separately for the client state machine and server state machine, in sections 3.2.5.3 and 3.3.5.2.

*Date format: YYYY/MM/DD

[MS-SSTR]: Smooth Streaming Protocol

This topic lists the Errata found in the [MS-SSTR] document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 16, 2018 - Download

Errata below are for Protocol Document Version V8.0 – 2019/03/13.

Errata Published*	Description
2020/07/06	In Section 1.5 Prerequisites/Preconditions, added reference to the amendment for HEVC. Changed from: It is also assumed that the client is integrated with a higher-layer implementation that supports any media formats that are used and can otherwise play the media that is transmitted by the server.<1> <1> Section 1.5: The Smooth Streaming Protocol is supported… Changed to: It is also assumed that the client is integrated with a higher-layer implementation that supports any media formats that are used and can otherwise play the media that is transmitted by the server.<1><2> <1> Section 1.5: For requirements to enable cloud-based Smooth Streaming of High Efficiency Video Coding (HEVC) encoded video see the amendment for HEVC [MSDOCS-SSTR-HEVC]. <2> Section 1.5: The Smooth Streaming Protocol is supported…

*Date format: YYYY/MM/DD

[MS-SWN]: Service Witness Protocol

This topic lists the Errata found in [MS-SWN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

[MS-TCC]: Tethering Control Channel Protocol

This topic lists the Errata found in [MS-TCC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-TDS]: Tabular Data Stream Protocol

This topic lists the Errata found in [MS-TDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

March 20, 2017 - Download

August 21, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

October 14, 2019 - Download

June 15, 2020 - Download

June 1, 2021 - Download

[MS-TLSP]: Transport Layer Security (TLS) Profile

This topic lists the Errata found in [MS-TLSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

September 15, 2017 - Download

[MS-TPMVSC]: Trusted Platform Module (TPM) Virtual Smart Card Management Protocol

This topic lists the Errata found in [MS-TPMVSC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-TSCH]: Task Scheduler Service Remoting Protocol

This topic lists the Errata found in [MS-TSCH] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

[MS-TSGU]: Terminal Services Gateway Server Protocol

This topic lists the Errata found in [MS-TSGU] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

[MS-TSTS]: Terminal Services Terminal Server Runtime Interface Protocol

This topic lists the Errata found in [MS-TSTS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

April 7, 2021 - Download

[MS-TSWP]: Terminal Services Workspace Provisioning Protocol

This topic lists the Errata found in [MS-TSWP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-UAMG]: Update Agent Management Protocol

This topic lists the Errata found in [MS-UAMG] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

RSS
Atom

Errata are subject to the same terms as the Open Specifications documentation referenced.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-UCODEREF]: Windows Protocols Unicode Reference

This topic lists the Errata found in [MS-UCODEREF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-VAPR]: Virtual Application Publication and Reporting (App-V) Protocol

This topic lists the Errata found in [MS-VAPR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-VHDX]: Virtual Hard Disk v2 (VHDX) File Format

This topic lists the Errata found in [MS-VHDX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

April 7, 2021 - Download

April 29, 2022 – Download

[MS-W32T]: W32Time Remote Protocol

This topic lists the Errata found in [MS-W32T] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

This topic lists the Errata found in [MS-WCCE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 29, 2020 – Download

October 6, 2021 - Download

Errata below are for Protocol Document Version V47.0 – 2021/10/06.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/09/03</td><td>The following sections were changed or added. Please see the diff document for the details.

In Section 3.1.1.4.3.8 Certificate Requests in Pre-sign flow
Description: Added new top-level section for new Certificate requests in Pre-sign flow subsections that follow.

In Section 3.1.1.4.3.8.1 New Certificate Request for Pre-sign processing
Description: Added new section describing how a certificate request can be designated for Pre-sign certificate processing at the server. Provided behavior note indicating the OS support for Pre-sign certificate processing.

<pbn> Pre-sign certificate processing is supported by the operating systems specified in [MSKB-5017379] and [MSKB-5017381], each with its related KB article download installed.

In Section 3.1.1.4.3.8.2 New Certificate Request After Pre-sign Processing
Description: Added new section to describe processing at the client after receiving a response for a request with a Pre-sign flag.

Section 3.2.1.1.4 Configuration List
Description: Added a flag to the Configuration List table that determines whether Pre-sign processing is enabled at the server. Also added the dummy private key description to the table.

Changed from:
<table><tr><th>Data name</th><th>Data description</th></tr><tr><td>Config_CertificateTransparency_Info_Extension_Oid</td><td>A string value that the CA sets for the SignedCertificateTimestampList extension in the issued certificate. The default value is OID szOID_CT_CERT_SCTLIST (1.3.6.1.4.1.11129.2.4.2) [RFC6962].</td></tr></table>
Changed to:
<table><tr><th>Data name</th><th>Data description</th></tr></table></td></tr>
</table>

Errata Published*	Description

Config_CertificateTransparency_Info_Extension_Oid	A string value that the CA sets for the SignedCertificateTimestampList extension in the issued certificate. The default value is OID szOID_CT_CERT_SCTLIST (1.3.6.1.4.1.11129.2.4.2) [RFC6962].
Config_PreSignCert_Enabled	A flag that indicates whether Certificate Pre-sign processing is enabled at the server. The default value is FALSE (not enabled).
Signing_Dummy_Private_Key	Contains the dummy private key generated with the same public key algorithm and key size as the private key of the current CA signing certificate, as specified in section 3.2.1.1.2.

In Section 3.2.1.4.2.1.4.10 Processing Rules for Pre-sign Certificate Requests
Description: Added new top-level section for processing rules for Pre-sign certificate requests.

Section 3.2.1.4.2.1.4.10.1 New Certificate Request with Pre-sign flag
Description: Created new section to specify additional processing the CA MUST perform on Certificate Requests containing the Pre-sign flag.

Section 3.2.1.4.2.1.4.10.2 New Certificate Request without Pre-sign flag
Description: Created new section to specify certain processing that the Certificate Authority MUST perform on every new certificate request that does not have the Pre-sign flag set.

Section 3.2.1.4.3.1.1 dwFlags Packed Data Requirements
Description: Added a B bit to define the setting that indicates to the server that it MUST process the request as a new Pre-sign certificate request.

Changed from:
ExtendedFlags: This bit-field defines extended options for the server's request processing.

0	1	2	3	4	5	6	7
0	0	0	0	0	A	0	0

Where the bits are defined as follows:

Value	Description
A	If this bit is set, the server MUST process the request as a new Certificate Transparency request, in accordance with section 3.2.1.4.2.1.4.3.1.

Changed to:

ExtendedFlags: This bit-field defines extended options for the server's request processing.

0	1	2	3	4	5	6	7
0	0	0	0	B	A	0	0

Where the bits are defined as follows:

Value	Description
A	If this bit is set, the server MUST process the request as a new Certificate Transparency

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>request, in accordance with section 3.2.1.4.2.1.4.3.1.</td></tr>
<tr><td>B</td><td>If this bit is set, the server MUST process the request as a new Pre-sign certificate request, in accordance with section 3.2.1.4.2.1.4.10.1.</td></tr>
</table>
</td></tr>
<tr><td>2022/08/09</td><td>
In Section 3.2.1.1.1.2 Request Table Optional Data Elements:
Added 'Issuer_Name_Id' data element to the optional data elements request table.
Changed from:
".....
Request_Endorsement_Key_Hash
Request_Endorsement_Certificate_Hash"
Changed to:
".....
Request_Endorsement_Key_Hash
Request_Endorsement_Certificate_Hash
Issuer_Name_Id"
In Section 3.2.1.4.2.1.1.4 Storing Request Parameters in the Request Table
Added and defined the Issuer_Name_Id data element to the request parameters in the Request Table.
Changed from:
<table>
<tr><th>Column name</th><th>Processing rules</th></tr>
<tr><td>....</td><td>....</td></tr>
<tr><td>Request_Endorsement_Certificate_Hash</td><td>The CA MUST store the SHA2 hash of the trust module certificate used for attestation
from the certificate request as a hexadecimal string with no spaces.</td></tr>
</table>
Changed to:
<table>
<tr><th>Column name</th><th>Processing rules</th></tr>
<tr><td>....</td><td>....</td></tr>
<tr><td>Request_Endorsement_Certificate_Hash</td><td>The CA MUST store the SHA2 hash of the trust module certificate used for attestation from the certificate request as a hexadecimal string with no spaces.</td></tr>
<tr><td>Issuer_Name_Id</td><td>The CA MUST store the version information (section 3.2.1.4.3.2.39) of the current CA signing certificate as stored in the Signing_Cert_Certificate datum.</td></tr>
</table>
In Section 3.2.1.4.3.2.16, PropID = 0x00000010 (CR_PROP_CAXCHGCERTCHAIN) "CA Exchange Certificate Chain",
</td></tr>
</table>

Errata Published*	Description

	"The CA MUST follow the specified processing rule updates to process a client's request for the CA exchange certificate, its complete chain, and all relevant CRLs; which includes updated instructions for constructing a signed CMS message."
	
	Changed from:
	
	▪ If *PropIndex* parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client.
	▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15.
	▪ Construct a signed **CMS** message with the following fields:
	  ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData).
	  ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements:
	  ▪ version: See section [RFC3852], section 5.1.
	  ▪ digestAlgorithms: Same digest algorithm as was used to sign current CA's certificate stored in Signing_Cert_Certificate datum.
	  ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the eContentType set to the OID szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the eContent field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum.
	  ▪ certificates: Contains CA's certificate stored in the Signing_Cert_Certificate datum and its parent certificates. To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1.
	
	Changed to:
	
	▪ If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client.
	▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15.
	▪ Retrieve the Issuer_Name_Id from the request database by finding the row with the Certificate_Hash equal to the Current_CA_Exchange_Cert hash value.
	▪ Find the CA signing certificate corresponding to the Current_CA_Exchange_Cert by looking for an entry in the Signing_Cert table with the certificate index (section 3.2.1.4.3.2.39) matching the lower 16 bits of the Issuer_Name_Id value retrieved in step 3 of this procedure.91
	▪ Construct a signed CMS message with the following fields:
	  ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData).
	  ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements:
	  ▪ version: See section [RFC3852], section 5.1.
	  ▪ digestAlgorithms: Same digest algorithm as was used by the CA signing certificate retrieved in step 4 of this procedure, to sign the Current_CA_Exchange_Cert.
	  ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the eContentType set to the OID szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the eContent field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum.
	  ▪ certificates: Contains CA's certificate (1), as retrieved in step 4 of this procedure, and its parent certificates (1). To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1.
	
	[91] In some cases, the CA signing certificate with "certificate index" zero could be returned instead of the actual signing certificate that issued Current_CA_Exchange_Cert. This behavior can be automatically fixed by restarting certificate service whenever a new exchange certificate is created.
	In Section 3.2.1.4.3.2.33 PropID = 0x00000021 (CR_PROP_CAXCHGCERTCRLCHAIN) "CA Exchange Certificate Chain and CRL"

Errata Published*	Description
	"The CA MUST follow the specified processing rule updates to process a client's request for the CA exchange certificate, its complete chain, and all relevant CRLs; which includes updated instructions for constructing a signed CMS message." Changed from: ▪ ▪ If *PropIndex* parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. ▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. ▪ Construct a signed **CMS** message with the following fields: ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData). ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used to sign current CA's **certificate** stored in Signing_Cert_Certificate datum. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the **eContentType** set to the **OID** szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the **eContent** field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains CA's certificate stored in the Signing_Cert_Certificate datum and its parent certificates. To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. Changed to: ▪ If *PropIndex* parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. ▪ Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. ▪ Retrieve the **Issuer_Name_Id** from the request database by finding the row with the Certificate_Hash equal to the Current_CA_Exchange_Cert hash value. ▪ Find the CA signing certificate corresponding to the Current_CA_Exchange_Cert by looking for an entry in the Signing_Cert table with the **certificate index** (section 3.2.1.4.3.2.39) matching the lower 16 bits of the **Issuer_Name_Id** value retrieved in step 3 of this procedure.[95] ▪ Construct a signed **CMS** message with the following fields: ▪ ContentType: szOID_RSA_signedData (1.2.840.113549.1.7.2, id-signedData). ▪ Content: SignedData (as specified in [RFC3852], section 5.1) with the following requirements: ▪ version: See section [RFC3852], section 5.1. ▪ digestAlgorithms: Same digest algorithm as was used by the CA signing certificate retrieved in step 4 of this procedure, to sign the Current_CA_Exchange_Cert. ▪ encapContentInfo: EncapsulatedContentInfo structure (as specified in [RFC3852], section 5.2) with the **eContentType** set to the **OID** szOID_PKCS_7_DATA (1.2.840.113549.1.7.1, id-data) and the **eContent** field set to the CA's exchange certificate from the Current_CA_Exchange_Cert datum. ▪ certificates: Contains **CA's certificate (1)**, as retrieved in step 4 of this procedure, and its parent **certificates (1)**. ~~excluding the **root certificate**.~~ To obtain parent certificates, the CA SHOULD use Authority Information Access (AIA) extension of its certificate and its parent certificates. The AIA extension is specified in [RFC3280] section 4.2.2.1. [95] In some cases, the CA signing certificate with "certificate index" zero could be returned instead of the actual signing certificate that issued Current_CA_Exchange_Cert. This behavior can be automatically fixed by restarting certificate service whenever a new exchange certificate is created.

Errata Published*	Description
	In Section 3.2.1.4.3.2.39 PropID = 0x00000027 (CR_PROP_CACERTVERSION) "CA Signing Certificates Revisions" Bolded "version information" Changed from: The CA MUST return the array in a CERTTRANSBLOB (section 2.2.2.2) structure. Each ULONG value in the returned array MUST contain version information for a signing certificate in **little-endian** format. Changed to: The CA MUST return the array in a CERTTRANSBLOB (section 2.2.2.2) structure. Each ULONG value in the returned array MUST contain **version information** for a signing certificate in **little-endian** format.
2022/07/26	In Section 3.2.1.4.3.2.16 PropID = 0x00000010 (CR_PROP_CAXCHGCERTCHAIN) "CA Exchange Certificate Chain": Removed the statement 'excluding the root certificate' as actual server behavior does not exclude the root certificate in a CMS message. Changed from: "The client has requested the CA exchange certificate and its complete chain. The CA MUST follow these processing rules to process the client's request: 1. If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. 2. Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. 3. Construct a signed CMS message with the following fields: ▪ ContentType: ..... ▪ Content: ..... ▪ version: ..... ▪ digestAlgorithms: ..... ▪ encapContentInfo: ..... ▪ certificates: Contains CA's certificate (1) stored in the Signing_Cert_Certificate datum and its parent certificates (1) excluding the root certificate." Changed to: "The client has requested the CA exchange certificate and its complete chain. The CA MUST follow these processing rules to process the client's request: 1. If PropIndex parameter is not equal to 0x0 or 0xFFFFFFFF, return the E_INVALIDARG (0x80070057) error to the client. 2. Validate that the Current_CA_Exchange_Cert datum contains a current, valid CA exchange certificate by executing steps 2 and 3 in section 3.2.1.4.3.2.15. 3. Construct a signed CMS message with the following fields: ▪ ContentType: ..... ▪ Content: ..... ▪ version: ..... ▪ digestAlgorithms: ..... ▪ encapContentInfo: ..... ▪ certificates: Contains CA's certificate (1) stored in the Signing_Cert_Certificate datum and its parent certificates (1)."~~excluding~~

Errata Published*	Description
	~~the root certificate~~
2022/06/28	In Section 3.2.2.6.2.1.4.4.1 Flags Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1."
2022/06/14	In Section 3.2.2.6.2.1.4.4.1 Flags Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB If this flag is set and if the certificate (1) has been issued, the CA SHOULD NOT persist the information about the request in the Request table that is specified in section 3.2.1.1.1."
2022/05/10	Section 2.2.2.7.7.4 szOID_NTDS_CA_SECURITY_EXT Description: "Created new topic to define the szOID_NTDS_CA_SECURITY_EXT security extension for enhanced security protections. Also added operating system applicability [MSFT-CVE-2022-26931] for this security update." Changed From: "" Changed To:

Errata Published*	Description
	"OID = 1.3.6.1.4.1.311.25.2. Internal Name: szOID_NTDS_CA_SECURITY_EXT[11]. Description: Contains objectSid of the Active Directory object whose information is being used to construct the subject information of an issued certificate. The CA MUST consider this extension from request attributes only when the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set on the corresponding certificate template object. See section 3.2.2.6.2.1.4.5.9 for specifics on how the CA processes this extension. This extension value MUST be DER-encoded ([X690]). The critical field for this extension SHOULD be set to FALSE. szOID_NTDS_OBJECTSID: 1.3.6.1.4.1.311.25.2.1. Format: The following is the ASN.1 format ([X690]) for this attribute. OtherName ::= SEQUENCE { type-id szOID_NTDS_OBJECTSID, value octet string} [11]This security extension is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed." Section 2.3 Directory Service Schema Elements Description: Added 'objectSid' descriptor to the Computer class and User class lists in the Class/Attribute table. Changed From: "Computer cn distinguishedName dNSHostName objectGuid Changed To: "Computer cn distinguishedName dNSHostName objectGuid objectSid Changed From: "User cn

Errata Published*	Description
	distinguishedName objectGuid mail userCertificate userPrincipalName" Changed To: "User cn distinguishedName objectGuid objectSid mail userCertificate userPrincipalName" Section 3.2.2.1.2.1 Search Requests Description: "Added the attribute 'objectSid' to the list of attributes that the CA should use for an LDAP SearchRequest message." Changed From: ● mail ● objectGUID ● userPrincipalName Changed To: ● mail ● objectGUID ● objectSid ● userPrincipalName Section 3.2.2.1.3.1 Search Requests Description: Added the attribute 'objectSid' to the list of attributes that the CA should use for an LDAP SearchRequest message.

Errata Published*	Description
	Changed From: ● mail ● objectGUID ● userPrincipalName Changed To: ● mail ● objectGUID ● objectSid ● userPrincipalName Section 3.2.2.6.2.1.4.5.9 msPKI-Certificate-Name-Flag Description: "Enhanced the processing instructions to specify that the CA must add the new szOID_NTDS_CA_SECURITY_EXT security extension to the issued certificate when the CT_FLAG_NO_SECURITY_EXTENSION flag is not set; and to do the same when the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set and CT_FLAG_NO_SECURITY_EXTENSION is not set." Changed From: "4. If CT_FLAG_SUBJECT_REQUIRE_EMAIL is set, the CA MUST set the Subject field of the issued certificate (1) as a DN (1) whose E component value is obtained from the value of the mail attribute (1) of the requestor's user object in the working directory (1). For this, the CA MUST invoke the processing rules in section 3.2.2.1.2 with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name (1) and retrieve the mailattribute (1) from the returned EndEntityAttributes output parameter." Changed To: "4. If CT_FLAG_SUBJECT_REQUIRE_EMAIL is set, the CA MUST set the Subject field of the issued certificate (1) as a DN (1) whose E component value is obtained from the value of the mail attribute (1) of the requestor's user object in the working directory (1). For this, the CA MUST invoke the processing rules in section 3.2.2.1.2 with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name (1) and retrieve the mail attribute (1) from the returned EndEntityAttributes output parameter. 5. If the CT_FLAG_NO_SECURITY_EXTENSION flag is not set, the CA MUST add the szOID_NTDS_CA_SECURITY_EXT security extension, as specified in section 2.2.2.7.7.4, to the issued certificate with the value set to the string format of the objectSid attribute obtained from the requestor’s user object in the working directory. For this, the CA MUST invoke the processing rules in section 3.2.2.1.2, with input parameter EndEntityDistinguishedName set equal to the requester's user object distinguished name, and retrieve the objectSid attribute from the returned EndEntityAttributes output parameter." Changed From: "3. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set, then the CA MUST use the subject and subject alternative name information provided in the certificate (1) request. If no subject name is

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>provided in the request, the CA MUST reject the request."

Changed To:

"3. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set, then the CA MUST use the subject and subject alternative name information provided in the certificate (1) request. If no subject name is provided in the request, the CA MUST reject the request.

4. If CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set and CT_FLAG_NO_SECURITY_EXTENSION is not set, then the CA MUST add the szOID_NTDS_CA_SECURITY_EXT security extension (section 2.2.2.7.7.4) to the issued certificate, that is, if it is provided as an extension in the request."</td></tr>
<tr><td>2022/05/10</td><td>In Section 3.2.2.6.2.1.4.5.6 msPKI-Enrollment-Flag

Description: Updated client processing instructions to indicate that the CA MUST also enforce the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag when the conditions specified in new section 3.2.2.6.2.1.4.8 are met.
Also revised client processing instructions to specify the conditions under which the subject alternative name (SAN) extension MUST be added to the new certificate being issued.

Changed From:

<table><tr><th>Flag</th><th>Client processing</th></tr><tr><td>0x00000040
CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT</td><td>The CA MUST enforce this flag only for certificate renewal requests.</td></tr></table>If this flag is set in the template:
● The CA MUST NOT enforce the signature processing rules specified for the following attributes: msPKI-RA-Signature, msPKI-RA-Policies, and msPKI-Application-Policy.
● The CA MUST ignore the CT_FLAG_PEND_ALL_REQUESTS flag.

Changed To:

<table><tr><th>Flag</th><th>Client processing</th></tr><tr><td>0x00000040
CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT</td><td>The CA MUST enforce this flag only for certificate renewal requests and only when the conditions specified in section 3.2.2.6.2.1.4.8 are met.</td></tr></table>If this flag is set in the template:
● The CA MUST NOT enforce the signature processing rules specified for the following attributes: msPKI-RA-Signature, msPKI-RA-Policies, and msPKI-Application-Policy.
● The CA MUST ignore the CT_FLAG_PEND_ALL_REQUESTS flag.
● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT is set and the old certificate, based on which reenrollment is occurring, contains the subject alternative name (SAN) extension, then the same SAN extension MUST be added to the new certificate being issued.</td></tr>
</table>

Errata Published*	Description
	In Section 3.2.2.6.2.1.4.8 CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT Enforcement Conditions Description: Created new topic to specify the conditions that are required to be met before enforcing the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag, that is, if the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag is set in the template. Changed From: "" Changed To: "If the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag is set in the template, the CA MUST verify that all the following conditions are satisfied before enforcing the CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT flag: ● The old certificate, based on which the reenrollment is occurring, MUST contain the Certificate Template OID extension, as specified in section 2.2.2.7.7.2. ● The TemplateID from the old certificate MUST match the TemplateID of the current template. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is set, then the CA MUST verify that subject name is supplied in the request, and that it matches with the subject of the old certificate. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, then the old certificate MUST contain the subject alternative name (SubjectAltName) extension. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, then the SubjectAltName extension from the old certificate MUST contain either an rfc822Name or otherName with OID szOID_NT_PRINCIPAL_NAME (1.3.6.1.4.1.311.20.2.3). ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set and the SubjectAltName contains otherName, then the value of otherName MUST match the value of the userPrincipalName attribute from the requestor's user object in the working directory. ● If the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag is not set, and the SubjectAltName contains the rfc822Name, then the value of rfc822Name MUST match the value of the mail attribute from the requestor's user object in the working directory."

*Date format: YYYY/MM/DD

[MS-WCFESAN]: WCF-Based Encrypted Server Administration and Notification Protocol

This topic lists the Errata found in [MS-WCFESAN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS

Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-WDHCE]: Wi-Fi Display Protocol Hardware Cursor Extension

This topic lists the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 29, 2022 – Download

[MS-WDSMT]: Windows Deployment Services Multicast Transport Protocol

This topic lists the Errata found in [MS-WDSMT] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WDSOSD]: Windows Deployment Services Operation System Deployment Protocol

This topic lists the Errata found in the MS-FAX document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

September 12, 2018 - Download

[MS-WFDAA]: Wi-Fi Direct (WFD) Application to Application Protocol

This topic lists the Errata found in [MS-WFDAA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

[MS-WFDPE]: Wi-Fi Display Protocol Extension

This topic lists the Errata found in [MS-WFDPE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

March 20, 2017 - Download

June 1, 2017 - Download

[MS-WKST]: Workstation Service Remote Protocol

This topic lists the Errata found in [MS-WKST] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V31.0 – 2022/04/29.

Errata Published*	Description
2022/09/03	In Section 2.2.5.19, JOINPR_ENCRYPTED_USER_PASSWORD_AES, corrected typo: Changed from: AuthDate: 64 bytes, the HMAC. Changed to: AuthData: 64 bytes, the HMAC. In Section 2.2.5.19.3, Encrypt Key and MAC Key, clarified the calculation of the keys: Changed from: The following variables and values are used in calculating the EncryptKey and HMACKey values. versionbyte = 0x01 versionbyte_len = 1 algorithmString = "AEAD-AES-256-CBC-HMAC-SHA512" EncryptKey and MACKey are calculated as follows: EncryptKey := HMAC-SHA-512(SessionKey, "Microsoft WKST encryption key" + algorithmString +Length(SessionKey)) MACKey := HMAC-SHA-512(SessionKey, "Microsoft WKST MAC key" + algorithmString +Length(SessionKey)) Note that the SessionKey is calculated as in section 2.2.5.19.2. See [RFC4868] for details of the HMAC-SHA-512 algorithm. Changed to: The following variables and values are used in calculating the EncryptKey and MACKEY values: Constant/value | Description

Errata Published*	Description

versionbyte 0x01	Version identifier.
versionbyte_len 1	Version identifier length.
WKST_AES_256_ALG "AEAD-AES-256-CBC-HMAC-SHA512"	A NULL terminated ANSI string.
WKST_AES256_ENC_KEY_STRING "Microsoft WKST encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.
WKST_AES256_MAC_KEY_STRING "Microsoft WKST MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.
WKST_AES256_ENC_KEY_STRING_LENGTH sizeof(WKST_AES256_ENC_KEY_STRING) (62)	The length of WKST_AES256_ENC_KEY_STRING, including the null terminator.
WKST_AES256_MAC_KEY_STRING_LENGTH sizeof(WKST_AES256_MAC_KEY_STRING) (55)	The length of WKST_AES256_MAC_KEY_STRING, including the null terminator.

EncryptKey and MACKey are calculated as follows:

EncryptKey := HMAC-SHA-512(SessionKey, WKST_AES256_ENC_KEY_STRING)

MACKey := HMAC-SHA-512(SessionKey, WKST_AES256_MAC_KEY_STRING)

Note that the SessionKey is calculated as in section 2.2.5.19.2. See [RFC4868] for details of the HMAC-SHA-512 algorithm.

In Section 2.2.5.19.4, Encrypt Encoded Password, clarified the encreyption process:

Changed from:

Encrypt the encoded password as follows:

Salt := Randomly generated 16 bytes

Cipher := AES-CBC(EncryptKey[0:256], IV, EncodedPasswordLength(4 bytes) + EncodedPassword)

AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte_len)

Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.

Changed to:

Encrypt the encoded password as follows:

Salt := Randomly generated 16 bytes

Encoded_Plaintext:= EncodedPasswordlength (4 bytes) + EncodedPassword.

Cipher := AES-CBC(EncryptKey[0:256], IV, Encoded_Plaintext)

AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte_len)

Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.

Note that EncryptKey is truncated to 32 bytes and the entire 64-byte MACKey is used.

*Date format: YYYY/MM/DD

[MS-WMIO]: Windows Management Instrumentation Encoding Version 1.0 Protocol

This topic lists the Errata found in [MS-WMIO] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

April 7, 2021 - Download

[MS-WMF]: Windows Metafile Format

This topic lists the Errata found in [MS-WMF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

April 7, 2021 - Download

[MS-WPO]: Windows Protocols Overview

This topic lists the Errata found in [MS-WPO] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WSDS]: WS-Enumeration Directory Services Protocol Extensions

This topic lists the Errata found in [MS-WSDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 20, 2017 - Download

June 1, 2017 - Download

[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista

This topic lists the Errata found in [MS-WSMV] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

December 1, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

[MS-WSP]: Windows Search Protocol

This topic lists the Errata found in [MS-WSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

[MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions

This topic lists the Errata found in [MS-WSTEP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

Errata below are for Protocol Document Version V14.0 – 2021/06/25.

Errata Published*	Description
2021/09/21	In Section 3.1.4.1.3.2 wst:RequestedSecurityTokenType, updated to clarify the RequestSecurityTokenResponseCollection and RequestedSecurityToken element responses, the certificate locations, and the BinarySecurityToken format and value type. Changed from: "The WSTEP extends wst: RequestedSecurityTokenType with two additional elements. ● <xs:element ref="wsse:BinarySecurityToken" /> ● <xs:element ref="wsse:SecurityTokenReference" /> wsse:BinarySecurityToken: The wsse:BinarySecurityToken element contains the issued certificate. The issued certificate follows the encoding and data structure defined in [MS-WCCE] section 2.2.2.8." Changed to: "MS-WSTEP extends the wst: RequestedSecurityTokenType with two additional elements as follows. ● <xs:element ref="wsse:BinarySecurityToken" /> ● <xs:element ref="wsse:SecurityTokenReference" /> The server SHOULD<2> include the end entity certificate in the RequestedSecurityTokenresponse. The ValueType of the BinarySecurityToken element for this RequestedSecurityToken response MUST be X509v3 [RFC5280]. The server MUST also include a CMC full PKI response in the RequestSecurityTokenResponseCollection, as specified in sections 4.2 and 4.3 of [WSTrust1.3]. wsse:BinarySecurityToken: The wsse:BinarySecurityToken element contains the issued certificatein either a full CMC response or as a stand alone x509v3 certificate[RFC5280]. <2> Section 3.1.4.1.3.2: Microsoft Windows always includes the requested end entity certificate in the RequestedSecurityToken."

*Date format: YYYY/MM/DD

[MS-WSUSAR]: Windows Server Update Services: Administrative API Remoting Protocol

This topic lists the Errata found in the MS-WSUSAR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

March 4, 2020 - Download

April 7, 2021 - Download

[MS-WSUSOD]: Windows Server Update Services Protocols Overview

This topic lists the Errata found in [MS-WSUSOD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

[MS-WSUSSS]: Windows Update Services: Server-Server Protocol

This topic lists the Errata found in the [MS-WSUSSS] document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-WUSP]: Windows Update Services: Client-Server Protocol

This topic lists the Errata found in [MS-WUSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

March 4, 2020 - Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V33.0 – 2022/04/29.

Errata Published *	Description
2022/09/20	Section 2.2.2.2.6 GetExtendedUpdateInfo Description: Updated product behavior note 25 to read: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed. Changed from: The GeoId property is supported in the down-level operating systems specified in [MSKB-5005101], each with its related KB article download installed. It is also supported on Windows 11 v22H2 and later. Changed to: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed. Section 3.1.1.1 Populating the Data Model Description: Updated product behavior note 36 to read: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed. Changed from:

Errata Published *	Description
	The GeoId property is supported on the down-level operating systems specified in [MSKB-5005101], each with its related KB article download installed. It is also supported on Windows 11 v22H2 and later. Changed to: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed.
2022/07/26	Changed from: The SOAP operation is defined as follows. <wsdl:operation name="GetExtendedUpdateInfo2"> <soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /> Changed to: <soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" />
2022/07/12	In Section 2.2.2.2.10 GetExtendedUpdateInfo2, removed additional statement '<wsdl:operation name="GetExtendedUpdateInfo2">' from SOAP operation definition. Changed from: The SOAP operation is defined as follows. <wsdl:operation name="GetExtendedUpdateInfo2"> <soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /> Changed to: <soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" />

*Date format: YYYY/MM/DD

[MS-XCA]: Xpress Compression Algorithm

This topic lists the Errata found in [MS-XCA] since it was last published.

Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS

Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 4, 2020 - Download

August 24, 2020 – Download

[MS-XCEP]: X.509 Certificate Enrollment Policy Protocol

This topic lists the Errata found in [MS-XCEP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download