[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

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

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/09/20</td><td>
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:
<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>
Changed to:
<table>
<tr><th>Constant Name</th><th>Meaning</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>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<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 section</td></tr>
<tr><td>2.2.2.7 LSAPR_REVISION_INFO</td><td>Created new section</td></tr>
<tr><td>2.2.7.2 TRUSTED_INFORMATION_CLASS</td><td>Updated</td></tr>
<tr><td>2.2.7.3 LSAPR_TRUSTED_DOMAIN_INFO</td><td>Updated</td></tr>
<tr><td>2.2.7.21 LSA_FOREST_TRUST_RECORD</td><td>Updated</td></tr>
<tr><td>2.2.7.22 LSA_FOREST_TRUST_RECORD_TYPE</td><td>Updated</td></tr>
<tr><td>2.2.7.30 LSAPR_TRUSTED_DOMAIN_FULL_INFORMATION_INTERNAL_AES</td><td>Created new section</td></tr>
<tr><td>2.2.7.31 LSA_FOREST_TRUST_SCANNER_INFO</td><td>Created new section</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description	
	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