[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>

Copyright © 2022 Microsoft Corporation

Errata Published*	Description

Value	Description
A	DES-CBC-CRC
. . .	
I	Resource-SID-compression-disabled<12>
J	AES256-CTS-HMAC-SHA1-96-SK

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.

Copyright © 2022 Microsoft Corporation

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

Copyright © 2022 Microsoft Corporation