

[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.

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](#)

December 1, 2022 - [Download](#)

Errata below are for Protocol Document Version [V40.0 – 2022/12/01](#).

Errata Published*	Description
2023/03/06	<p>Section 5.1 Security Considerations for Implementers: Added statement to recommend strong vs. weak encryption usage.</p> <p>Changed from:</p> <p>5.1 Security Considerations for Implementers KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]).</p> <p>Changed to:</p> <p>5.1 Security Considerations for Implementers KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]).</p> <p>The encryption types AES128-CTC-HMAC-SHA1-96/AES256-CTC-HMAC-SHA1-96 or including AES256-CTS-HMAC-SHA1-96-SK if RC4 encryption types is selected is recommended. Setting RC4/DES only is weak and not recommended. For more information see section 2.2.7.</p>
2023/03/06	<p>Section 2.2.7 Supported Encryption Types Bit Flags: Added note to recommend strong vs. weak encryption usage.</p> <p>Changed from:</p>

Errata Published*	Description
	<p>AES256-CTS-HMAC-SHA1-96-SK: Enforce AES session keys when legacy ciphers are in use. When the bit is set, this indicates to the KDC that all cases where RC4 session keys can be used will be superseded with AES keys.</p> <p>All other bits MUST be set to zero when sent and MUST be ignored when they are received.</p> <p>Changed to:</p> <p>AES256-CTS-HMAC-SHA1-96-SK: Enforce AES session keys when legacy ciphers are in use. When the bit is set, this indicates to the KDC that all cases where RC4 session keys can be used will be superseded with AES keys.</p> <p>Note: The encryption types AES128-CTC-HMAC-SHA1-96/AES256-CTC-HMAC-SHA1-96 or including AES256-CTS-HMAC-SHA1-96-SK if RC4 encryption types is selected is recommended. Setting RC4/DES only is weak and not recommended.</p> <p>All other bits MUST be set to zero when sent and MUST be ignored when they are received.</p>

*Date format: YYYY/MM/DD