[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

August 24, 2020 – Download

Errata below are for Protocol Document Version V36.0 - 2020/08/26

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/10/26</td><td>In Section 3.4.5.4.1 Kerberos Binding of GSS_WrapEx(), updated the H1 HMAC algorithm.
Changed from:
where
(C1, newIV) = E(Ke, conf | plaintext | pad, oldstate.ivec)
H1 = HMAC(Ki, conf | plaintext+encrypted-data | pad)
Changed to:
where
(C1, newIV) = E(Ke, conf | plaintext | pad, oldstate.ivec)
H1 = HMAC(Ki, conf | plaintext | pad)</td></tr>
</table>

*Date format: YYYY/MM/DD