[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

Errata below are for Protocol Document Version V25.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/10/12</td><td>
<p>In Sections 3.1.1, Abstract Data Model, and 3.1.5.5.2, Key Used in the Cryptobinding HMAC-SHA1-160 Operation, the length of the TunnelKey has been updated to 60 octets to match observed behavior:</p>
<p>TunnelKey: The PEAP Tunnel Key (TK) is a 60-octet key generated as specified in section 3.1.5.5.2.1. This variable is used while generating Cryptobinding TLVs (section 3.1.5.5) and, if using cryptobinding, the final MPPE keys (section 3.1.5.7).</p>
<p>Tunnel key (TK): A 60-octet key generated by phase 1 of PEAP. For details, see section 3.1.5.5.2.1. The generated Tunnel Key is stored in the variable TunnelKey.</p>
<p>In Section 3.1.5.7, Key Management, the derivation of the keys from the Key_Material element in [RFC5216] has been updated to the text below to eliminate references to the TunnelKey ADM element for the case where one endpoint does not accept cryptobinding TLVs.</p>
<p>2. When an endpoint (either a PEAP server or PEAP peer) is incapable of sending cryptobinding TLVs, and the other endpoint is configured to accept such authentications, then the keys are obtained from the first 64 octets of the Key_Material, as specified in [RFC5216]: TLS-PRF-128 (master secret, "clientEAP encryption", client.random || server.random).</p>
<table>
<tr><th></th><th>First 32 bytes of Key_Material</th><th>Second 32 bytes of Key_Material</th></tr>
<tr><td>PEAP peer</td><td>MS-MPPE-Send-Key</td><td>MS-MPPE-Recv-Key</td></tr>
<tr><td>PEAP server</td><td>MS-MPPE-Recv-Key</td><td>MS-MPPE-Send-Key</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD