[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)

This topic lists the Errata found in [MS-SSTP] 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 V19.0 – 2021/04/07.

Errata Published*	Description
2021/05/17	In Section 3.2.5.2.2, Key Used in the Crypto Binding HMAC-SHA1-160 Operation, updated key generation description: Changed from: First, a 32-byte long string is generated from keys that are provided by the higher-layer PPP authentication method. This key is sent to the SSTP layer as part of the Inner Authentication Completed Event. If the higher-layer PPP authentication method generates Microsoft Point-to-Point Encryption (MPPE) keys, as specified in [RFC3079], then an implementation MUST obtain the HLAK by using the following method: • For MS-CHAPv2, as specified in [RFC2759]: SSTP Client HLAK = MasterSendKey | MasterReceiveKey, and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where | indicates concatenation of strings, and MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 3. • For EAPTLS, as specified in [RFC2716]: SSTP Client HLAK = MasterSendKey | MasterReceiveKey, and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where | indicates concatenation of strings and MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 4. • For EAP (other than EAPTLS), as specified in [RFC2284]: SSTP Client HLAK = Client Master Session Key (MSK), as specified in [RFC3748], and: SSTP Server HLAK = Server Master Session Key (MSK), as specified in [RFC3748]. If the HLAK is more than 32 octets, then the first 32 octets form the HLAK. If the HLAK is less than 32 octets, then the string is padded with 0x00 at the end to obtain a total length of 32 octets. Changed to:

Errata Published*	Description
	First, a 32-byte long string is generated from keys that are provided by the higher-layer PPP authentication method. This key is sent to the SSTP layer as part of the Inner Authentication Completed Event. This is also the case for EAP TLS. If the higher-layer PPP authentication method generates Microsoft Point-to-Point Encryption (MPPE) keys, as specified in [RFC3079], then an implementation MUST obtain the HLAK by using the following method: ● For MS-CHAPv2, as specified in [RFC2759]: SSTP Client HLAK = MasterSendKey | MasterReceiveKey, and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where | indicates concatenation of strings, and MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 3. ● For EAP-TLS, as specified in [RFC5216]:<8> SSTP Client HLAK = Client MasterSendKey, and: SSTP Server HLAK = Client MasterReceiveKey, where MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 4. ● For EAP (other than EAP-TLS), as specified in [RFC2284]: SSTP Client HLAK = Client Master Session Key (MSK), as specified in [RFC3748], and: SSTP Server HLAK = Server Master Session Key (MSK), as specified in [RFC3748]. If the HLAK is more than 32 octets, then the first 32 octets form the HLAK. Note that this covers EAP-TLS as well because the EAP TLK master session key is at least 64 bytes (see [RFC5247]). If the HLAK is less than 32 octets, then the string is padded with 0x00 at the end to obtain a total length of 32 octets. In Section 3.2.5.2.4, Key Used in the Crypto Binding HMAC-SHA256-256 Operation, updated key generation description: Changed from: First, a 32-byte long string is generated from keys that are provided by the higher-layer PPP authentication method. This key is sent to the SSTP layer as part of the Inner Authentication Completed Event.- If the higher-layer PPP authentication method generates Microsoft Point-to-Point Encryption (MPPE) keys, as specified in [RFC3079], then an implementation MUST obtain the HLAK using the following method: ● For MS-CHAPv2, as specified in [RFC2759]: SSTP Client HLAK = MasterSendKey | MasterReceiveKey and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where | indicates concatenation of strings and MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 3. ● For EAPTLS, as specified in [RFC2716]:

Errata Published*	Description
	SSTP Client HLAK = MasterSendKey | MasterReceiveKey and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 4 and where | indicates concatenation of strings. If the HLAK is more than 32 octets, then the first 32 octets form the HLAK. If the HLAK is less than 32 octets, then the string is padded with 0x00 at the end to obtain a total length of 32 octets. Changed to: First, a 32-byte long string is generated from keys that are provided by the higher-layer PPP authentication method. This key is sent to the SSTP layer as part of the Inner Authentication Completed Event. This is also the case for EAP-TLS. If the higher-layer PPP authentication method generates Microsoft Point-to-Point Encryption (MPPE) keys, as specified in [RFC3079], then an implementation MUST obtain the HLAK using the following method: ● For MS-CHAPv2, as specified in [RFC2759]: SSTP Client HLAK = MasterSendKey | MasterReceiveKey and: SSTP Server HLAK = MasterReceiveKey | MasterSendKey, where | indicates concatenation of strings and MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 3. ● For EAP-TLS, as specified in [RFC5216]:<9> SSTP Client HLAK = Client MasterSendKey, and: SSTP Server HLAK = Client MasterReceiveKey, where MasterSendKey and MasterReceiveKey are as specified in [RFC3079] section 4. If the HLAK is more than 32 octets, then the first 32 octets form the HLAK. Note that this covers EAP-TLS as well because, the EAP TLK master session key is at least 64 bytes (see [RFC5247]). If the HLAK is less than 32 octets, then the string is padded with 0x00 at the end to obtain a total length of 32 octets.

*Date format: YYYY/MM/DD