Handling Large Certificates and Long Certificate Chains in EAP-TLS

draft-ms-emu-eaptlscert-01

EMU IETF 103, Bangkok, November 2018, John Mattsson
Changes between draft-ms-emu-eapTLScert-00 and -01

• Updated according to the discussions and suggestions at IETF 102:
  • Re-organization of the text to distinguish which recommendations require changing certificates, and which require changing code.
  • New text describing that “Cached Information Extension” can help when roaming and authentication have already been done “home” network.
  • New text describing that updating to TLS 1.3 can help to significantly reduce the number of messages exchanged for an EAP-TLS authentication.
  • Placeholder for text on “Guidelines for certificates”
  • Editorial changes

We are soliciting text on guidelines for certificates used in EAP-TLS.
New document structure:

4. Handling of Large Certificates and Long Certificate Chains
   4.1. Updating Certificates
   4.2. Updating Code
   4.3. Guidelines for certificates

In Section 4.1 we look at recommendations that require an update of the certificates that are used for EAP-TLS authentication without requiring changes to the existing code base.

In Section 4.2 we look at recommendations that rely on updates to the EAP-TLS implementations which can be deployed with existing certificates.

Finally, in Section 4.3, we provide some guidelines when issuing certificates for use with EAP-TLS.
WANTED

REVIEWS

FEEDBACK