Handling Large Certificates and Long Certificate Chains in EAP-TLS

draft-ms-emu-eaptlscert-01

EMU IETF 103, Bangkok, November 2018, John Mattsson

emu by Jon Bunting https://www.flickr.com/photos/84744710@N06/14766013011

DRAFT-MS-EMU-EAPTLSCERT-01

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.

DRAFT-MS-EMU-EAPTLSCERT-01

- **New document structure:**
  -

- 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 bas
- 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