



Handling Large Certificates and Long Certificate Chains in TLS-based EAP Methods draft-ms-emu-eaptlscert-02

EMU IETF 104, Prague, March 2018, John Mattsson

DRAFT-MS-EMU-EAPTLS CERT-02



- Editorial reformulation and restructuring.
- **New document structure:**
 - 4. Handling of Large Certificates and Long Certificate Chains .
 - 4.1. Updating Certificates and Certificate Chains
 - 4.1.1. Guidelines for certificates
 - 4.2. Updating TLS and EAP-TLS Code
 - 4.2.1. Pre-distributing and Omitting CA Certificates
 - 4.2.2. Caching Certificates
 - 4.2.3. Compressing Certificates
 - 4.3. Updating Authenticators (Access Points)
- Section 4.1.1 Guidelines for certificates with text written by Sean Turner (new co-author).
 - Object Identifiers, DirectoryString and GeneralName types, Extensions.
- Section 4.2 divided into subsection for different approaches that require code updates.
- Section 4.3 that will shortly say why updating access points is hard.

WANTED

REVIEWS

FEEDBACK

WG ADOPTION?

WORK IN TLS WG?

