Handling Large Certificates and Long Certificate Chains in TLS-based EAP Methods

draft-ms-emu-eaptlscert-03

EMU IETF 105, Montreal, July 2019, John Mattsson

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

DRAFT-MS-EMU-EAPTLSCERT-03

- Changed “40 – 50 packets” to ”40 – 50 round-trips”
- Added short text about ”other TLS-based EAP methods” in the introduction
- New Section 4.2.4. Suppressing Intermediate Certificates
  - Describes the new draft draft-thomson-tls-sic-00 "Suppressing Intermediate Certificates in TLS” that defines a mechanism where a TLS client can inform a TLS server that it has all intermediate certificates and that the server can omit sending intermediates, thereby reducing the size of the TLS handshake.
- Added text to Section 4.3. Updating Authenticators
  - Describes why authenticators may want to limit the number of round-trips/packets/bytes that can be sent (avoid infinite loops, limit communication from unauthenticated devices, prevent denial-of-service attacks) and why updating the millions of already deployed access points and switches is in many cases not realistic.

WANTED

WG ADOPTION

REVIEWS