Using EAP-TLS with TLS 1.3
draft-ietf-emu-eap-tls13-07

EMU IETF 106, Singapore, John Preuß Mattsson
• Changes between draft-ietf-emu-eap-tls13-05 and draft-ietf-emu-eap-tls13-06
  • Change the application data in commit messages from 0x (empty string) to 0x00.
  • Added that EAP servers MUST send 0x00 and EAP peer MUST accept any application data as a commit message.
  • Added text and a new figure showing commit in separate EAP-Request.

• Changes between draft-ietf-emu-eap-tls13-06 and draft-ietf-emu-eap-tls13-07
  • The application data message is called “Commitment Message”
  • Added text and privacy considerations on padding.
  • Clarifications and references to RFC 8446
  • Added reference to draft-ietf-emu-eap-tls-cert
EAP-TLS 1.3 with PSK

- Request for not forbidding external PSKs in EAP-TLS by Tuomas Aura during WGLC:
  - EAP-PSK does not provide identity protection and perfect forward secrecy.
  - EAP-Pwd requires a PAKE:
    - IoT deployments may not implement all side-channel protections. IoT devices may want to reuse the underlying TLS implementation.
    - CFRG currently running a PAKE selection process.

- Some open issues (which have been discussed on the list):
  - Should EAP-TLS and EAP-TLS-PSK use the same method number and should they be specified in the same document?
  - Should a server allow authentication with both certificates and external PSKs?
  - Relationship of EAP identity and NAI when using external PSKs?
  - Should we distinguish external PSKs from resumption PSKs? Do we need to give guidance on external PSK identities?
WANTED

IETF LAST CALL

REVIEWS

IMPLEMENTATIONS