EAP-TLS with PSK Authentication (EAP-TLS-PSK)
draft-mattsson-emu-eap-tls-psk

EMU IETF Virtual Interim
John Preuß Mattsson, Mohit Sethi,
Tuomas Aura, Owen Friend
EAP-TLS 1.3 with PSK

• RFC 5216 section 2.1.1:
  • If the EAP server is not resuming a previously established session, then it MUST include a TLS server_certificate handshake message, and a server_hello_done handshake message MUST be the last handshake message encapsulated in this EAP-Request packet.
  • The certificate message contains a public key certificate chain for either a key exchange public key (such as an RSA or Diffie-Hellman key exchange public key) or a signature public key (such as an RSA or Digital Signature Standard (DSS) signature public key). In the latter case, a TLS server_key_exchange handshake message MUST also be included to allow the key exchange to take place.

• draft-ietf-emu-eap-tls13:
  • Pre-Shared Key (PSK) authentication SHALL NOT be used except for resumption.

• General consensus that PSK is desired and should be separate from EAP-TLS with certificates
EAP-TLS 1.3 with PSK

- Why use EAP-TLS-PSK:
  - 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 re-use the underlying TLS implementation.
    - CFRG currently running a PAKE selection process.
EAP-TLS 1.3 with PSK

Why use EAP-TLS-PSK:
- 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.

Is PSK the only other credential type with TLS:
- psk_ke / psk_dhe_ke
- tls_cert_withExtern_psk+psk_dhe_ke
- draft-vanrein-tls-kdh-06 (Quantum Relief with TLS and Kerberos)
- draft-tschofenig-tls-cwt-01 (Using CBOR Web Tokens (CWTs) in TLS and DTLS)
EAP-TLS 1.3 with PSK

- Different documents and EAP-types for different credentials (if and when they come to EMU)
  
  OR

- EAP-TLS-Everything-Other-Than-Basic-Client-and-Server-Certificates

- EAP-TLS-PSK only:
  - No need to add fragmentation support (save some resources for IoT deployments)
  - Can provide guidance on PSK identity and its relationship to NAI (draft-dt-tls-external-psk-guidance)
  - Can specify the role of resumption PSKs and server identity

- EAP-TLS-Everything-Other-Than-Basic-Client-and-Server-Certificates
  - Fewer documents and method types
  - Unclear how to provide exact guidance (on NAI for example)
  - Some TLS drafts might be moving targets
  - Less scope of tailoring implementations (getting rid of fragmentation)
WANTED

FEEDBACK

REVIEWS

IMPLEMENTATIONS