ERICSSON

USING EAP-TLS WITH TLS 1.3

DRAFT-MATTSSON-EAP-TLS13-02

IETF 101, EMU, MAR 19 2018

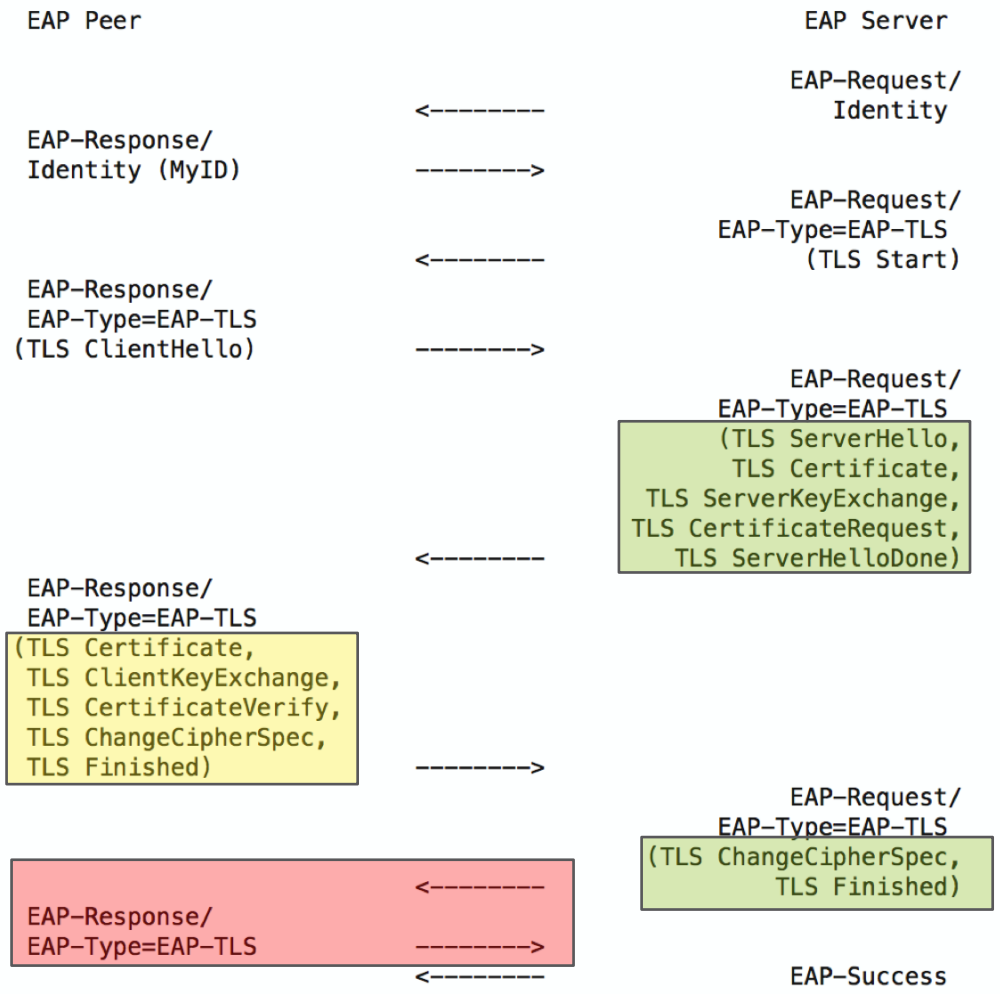
JOHN MATTSSON, MOHIT SETHI

DRAFT-MATTSSON-EAP-TLS13

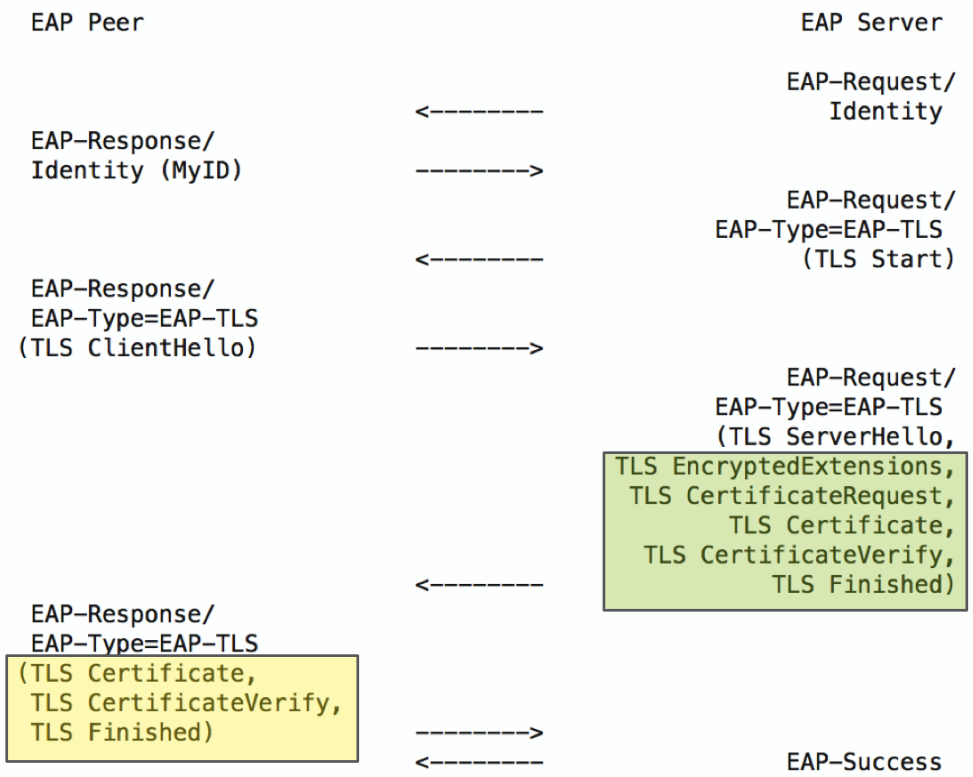
- EAP-TLS is widely supported for authentication in Wi-Fi. EAP-TLS is also the default mechanism for certificate based authentication in MulteFire and 3GPP 5G networks.
- TLS 1.3 is a complete remodeling of the TLS handshake protocol including a different message flow, different handshake messages, different key schedule, different cipher suites, different resumption, and different privacy protection.
  - This means that significant parts of the normative text in the previous EAP-TLS specification [RFC5216] are not applicable to EAP-TLS with TLS 1.3 (or higher).
- TLS 1.3 provides significantly improved security, privacy, and reduced latency when compared to earlier versions of TLS.
- Draft-mattsson-eap-tls13 updates RFC 5216: Specifies the use of EAP-TLS with TLS 1.3 while remaining backwards compatible with existing implementations of EAP-TLS.
  - Only lists additional and different requirements, restrictions, and processing compared to [I-D.ietf-tls-tls13] and [RFC5216].

NEW MESSAGE FLOW AND CONTENT

EAP-TLS with TLS 1.0, 1.1, or 1.2



EAP-TLS with TLS 1.3

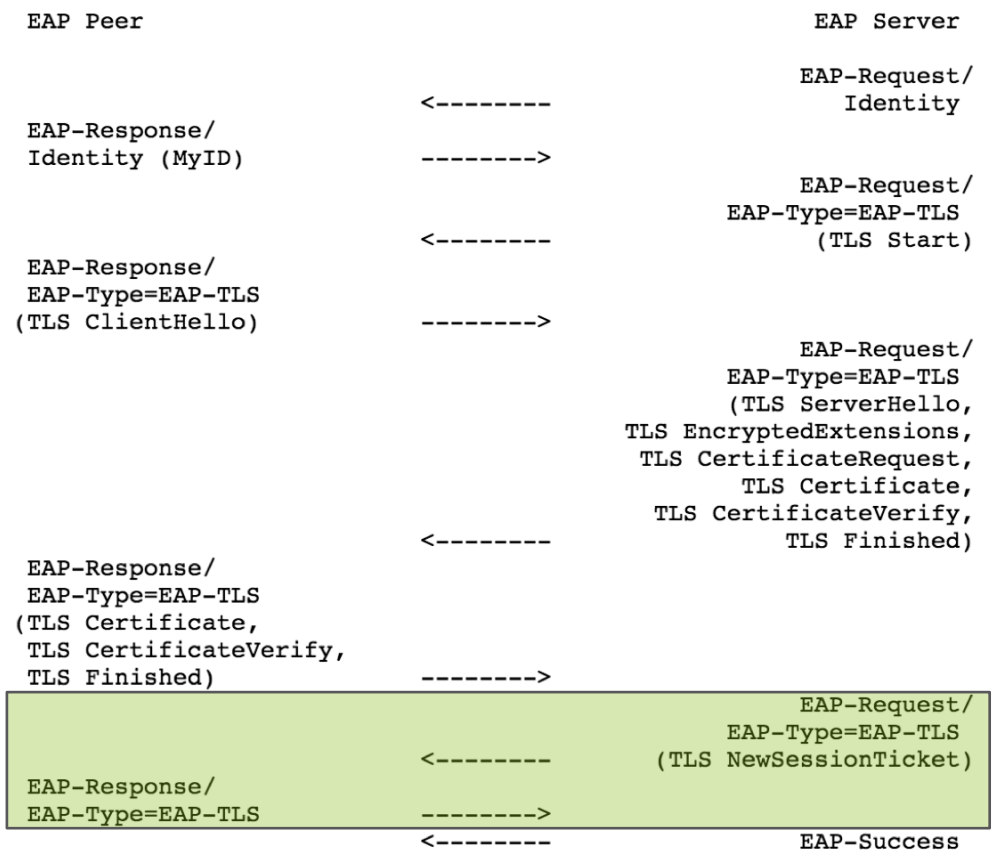


RESUMPTION

- TLS 1.3 replaces the session resumption mechanisms in earlier versions of TLS with a new PSK exchange.
- Pre-Shared Key (PSK) authentication SHALL NOT be used except for resumption.
- When using EAP-TLS with TLS 1.3, the EAP server MUST indicate support of resumption in the initial authentication.
  - To indicate support of resumption, the EAP server sends a NewSessionTicket message (containing a PSK and other parameters) after it has received the Finished message.
- If the client has received a NewSessionTicket message from the server, the client can use the PSK identity received in the ticket to negotiate resumption using the associated PSK.
- It is left up to the EAP peer whether to use resumption, but a EAP peer SHOULD use resumption as long as it has a valid ticket cached. An EAP server SHOULD accept resumption as long as the ticket is valid, but MAY require a full authentication.

RESUMPTION

EAP-TLS 1.3 ticket establishment



EAP-TLS 1.3 resumption

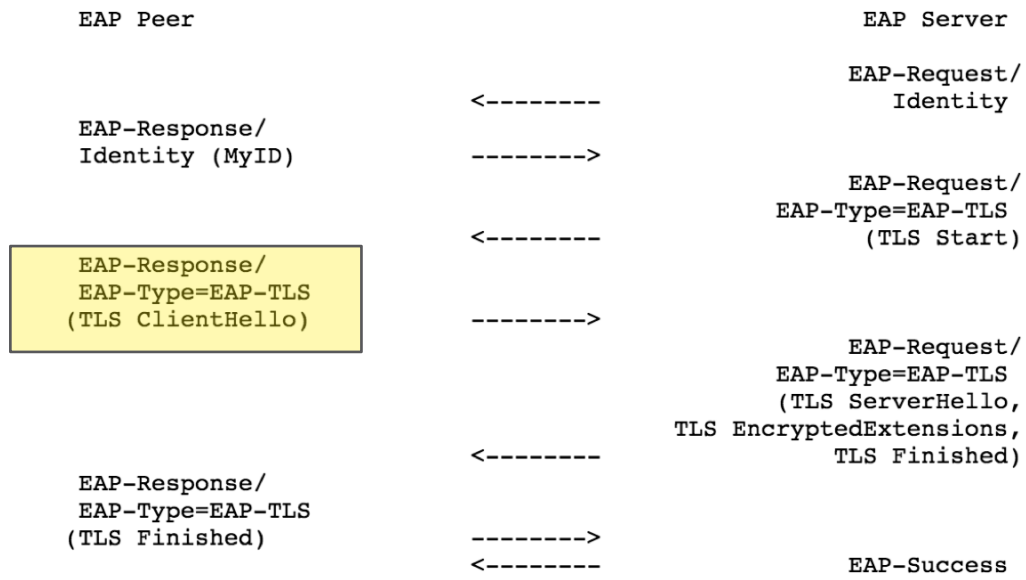
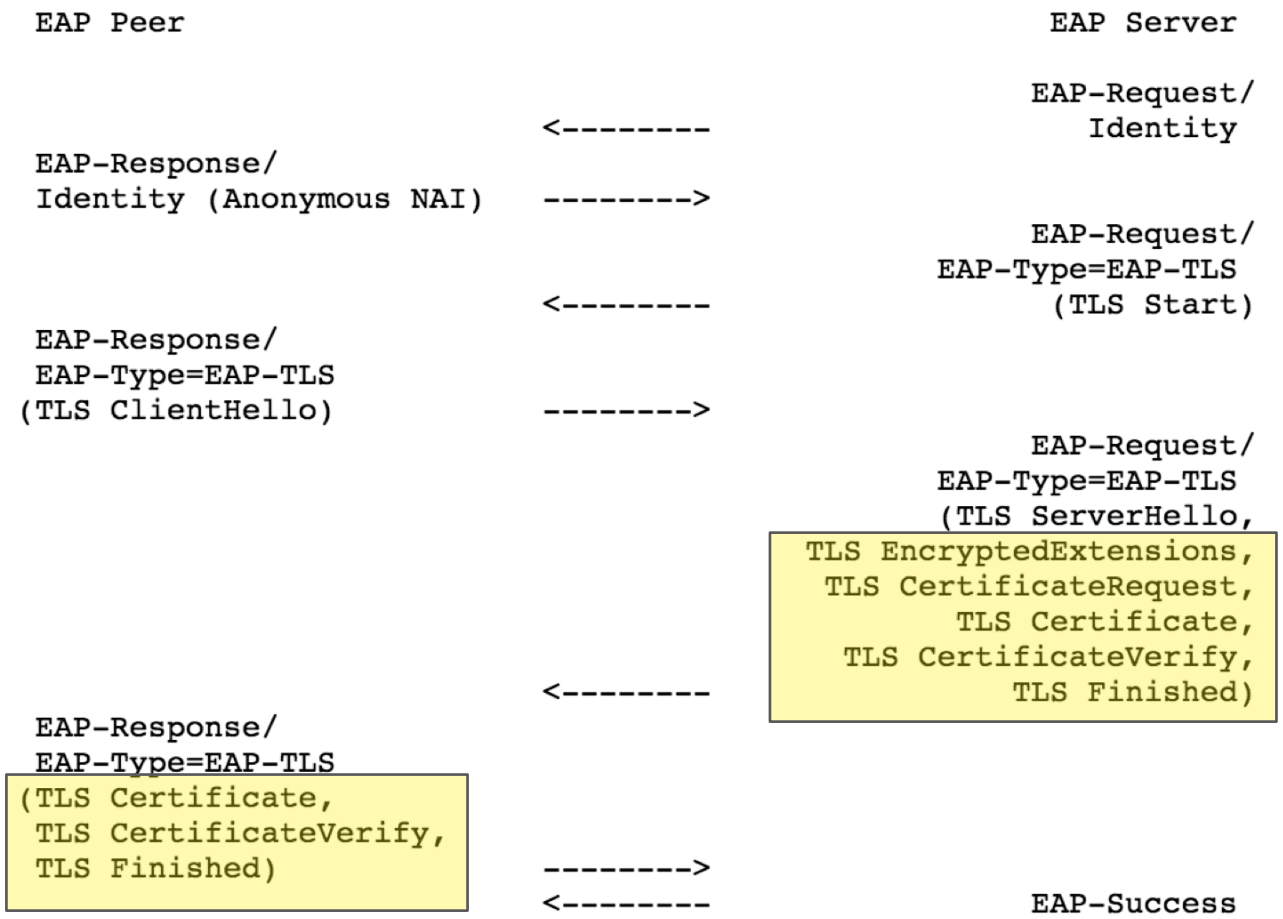


Figure 3: EAP-TLS resumption

PRIVACY

- TLS 1.3 increases and simplifies privacy by encrypting large parts of the TLS handshake including the certificate messages.
- There is therefore no need to send an empty certificate_list or perform a second handshake.
- EAP-TLS peer and server implementations supporting TLS 1.3 or higher MUST support anonymous NAIs and MUST confidentiality protect its identity (e.g. using Anonymous NAIs) when the EAP-TLS server is known to support TLS 1.3 or higher.
- What to do when server support of TLS 1.3 is unknown?



KEY HIERARCHY

- TLS 1.3 replaces the TLS pseudorandom function (PRF) used in earlier versions of TLS with HKDF and completely changes the Key Schedule.
- Specification needed to avoid non-interoperable implementations
- Suggested that when EAP-TLS is used with TLS version 1.3 or higher the Key_Material, IV, and Session-Id SHALL be derived from the exporter_master_secret using the TLS exporter interface:

```
Key_Material = TLS-Exporter("client EAP encryption KM", "", 128)
IV           = TLS-Exporter("client EAP encryption IV", "", 64)
Session-Id   = TLS-Exporter("client EAP encryption ID", "", 64)
```

- All other parameters such as MSK and EMSK are derived as specified in EAP-TLS [RFC5216], Section 2.3.

FRAGMENTATION

- Keep the sizes of client, server, and trust anchor certificates small and the length of the certificate chains short.
  - The use of ECC in certificates, signature algorithms, and groups are RECOMMENDED when using EAP-TLS with TLS 1.3 or higher.
  - An EAP-TLS deployment MAY further reduce the certificate sizes by limiting the number of Subject Alternative Names.
- Use mechanisms that reduce the sizes of Certificate messages.
  - Endpoints SHOULD reduce the sizes of Certificate messages by omitting certificates that the other endpoint is known to possess. When using TLS 1.3, all certificates that specifies a trust anchor may be omitted (see Section 4.4.2 of [I-D.ietf-tls-tls13]).
  - EAP-TLS peers and servers SHOULD support and use the Cached Information Extension as specified in [RFC7924].
  - EAP-TLS peers and servers MAY use other extensions for reducing the sizes of Certificate messages, e.g. certificate compression [I-D.ietf-tls-certificate-compression].

OTHER TLS 1.3 CHANGES

- The OCSP status handling in TLS 1.3 is different from earlier versions of TLS, see Section 4.4.2.1 of [I-D.ietf-tls-tls13]. In TLS 1.3 the OCSP information is carried in the CertificateEntry containing the associated certificate instead of a separate CertificateStatus message as in [RFC4366]. This enables sending OCSP information for all certificates in the certificate chain.
- TLS 1.3 strengthens the security claims for Confidentiality, Key strength, and Cryptographic Negotiation.
- TLS 1.3 cipher suites are defined differently than in earlier versions of TLS (see Section B.4 of [I-D.ietf-tls-tls13]), and the cipher suites discussed in Section 2.4 of [RFC5216] can therefore not be used when EAP-TLS is used with TLS version 1.3 or higher. When EAP-TLS is used with TLS version 1.3 or higher, the EAP-TLS peers and servers MUST comply with the requirements for the TLS version used.

MORE FEEDBACK!

IMPLEMENTATIONS!

WORKING GROUP ADOPTION?