6.2 TLS protocol profiles

6.2.1 General

The present clause contains the general 3GPP TLS profile. Other 3GPP specifications point to the present clause. Thus, parts of the present clause may also apply to devices and network nodes as specified in other specifications. New specifications using TLS should refer to this profile with as few exceptions as possible.

NOTE: DTLS 1.2 as specified in RFC 6347 [49] is based on TLS 1.2. Hence all requirements defined in this profile apply to DTLS protocol as well.

TLS end points shall support TLS with the following restrictions and extensions:

TLS versions

- SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 [67] and DTLS 1.0 shall not be supported.
- TLS 1.2 as specified in RFC 5246 [50] shall be supported. TLS 1.3 as specified in RFC 8446 [66] shall be supported. If DTLS is supported then DTLS 1.2 as specified in RFC 6347 [49] shall be supported.

Other

- If the TLS connection is used to transport HTTP over TLS as specified in RFC 2818 [52], then the client shall not establish a connection "upgraded to TLS Within HTTP/1.1" per RFC 2817 [53], but shall only establish the tunnel over a raw TCP connection.

6.2.2 Profiling for TLS 1.3

TLS 1.3 shall support the following restrictions and extensions:

TLS cipher suites and Diffie-Hellman groups

- The requirements given in section 9.1 of TLS 1.3 RFC 8446 [66] shall be followed. In addition:
  - Key exchange with secp384r1 should be supported.

TLS extensions

- The requirements given in section 9.2 of TLS 1.3 RFC 8446 [66] shall be followed. In addition:
  - The OCSP Status extention (a.k.a. certificate status request), as defined in RFC 6066 [57] and RFC 8466 [66] should be supported.

6.2.3 Profiling for TLS 1.2

TLS 1.2 (RFC 5246 [50]) shall support the following restrictions and extensions:

TLS cipher suites

- The rules on allowed cipher suites given in TLS 1.2 (RFC 5246 [50]) shall be followed.
- In addition, the following cipher suites are mandatory to support and recommended to use:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 [55]
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 [54]
- Support of the following cipher suites is recommended:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 [55]
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 [55]
- Only cipher suites with AEAD (e.g. GCM) and PFS (e.g. ECDHE, DHE) shall be supported.

Diffie-Hellman groups

- For ECDHE, the curve secp256r1 (P-256) as defined in RFC 8422 [71] shall be supported, secp384r1 (P-384) as defined in RFC 8422 [71] should be supported. Elliptic curve groups of less than 255 bits shall not be supported.

- For DHE, Diffie-Hellman groups of at least 4096 bits should be supported. Diffie-Hellman groups smaller than 2048 bits shall not be supported.

TLS hash algorithms and signature algorithms

- Hash algorithms: SHA-256 shall be supported. SHA-384 should be supported. MD5 and SHA-1 shall not be supported.

- Signature algorithms: ecdsa, rsa_pss_rsae, and rsa_pkcs1 shall be supported. Usage of rsa_pkcs1 is not recommended.

TLS compression

- The “null” compression method as specified in TLS 1.2 RFC 5246 [50] is mandatory to support. All other compression methods shall not be supported.

TLS extensions

- If TLS Extensions are used in conjunction with TLS, then for RFC 6066 [57] shall apply.

- The Server Name Indication (SNI) extension defined in RFC 6066 [57] shall be supported.

- The Truncated HMAC extension, defined in RFC 6066 [57] shall not be supported.

- TLS Session Resumption based on RFC 5246 [50] or RFC 5077 [59] should be supported.

- TLS servers and TLS clients shall support RFC 5746 [60]. The server shall accept client-initiated renegotiation only if secured according to RFC 5746 [60].

- The Extended Master Secret extension, defined in RFC 7627 [61] shall be supported.

- Signature Algorithms, defined in RFC 5246 [50] shall be supported.

- The Supported Groups extension, defined in RFC 8422 [71] and RFC 7919 [62] shall be supported.

- The OCSP Status (a.k.a. certificate status request) extention, defined in RFC 6066 [57] should be supported.

PSK cipher suites

- If pre-shared key (psk) cipher suites are implemented in TLS, then RFC 4279 [63] and RFC 5489 [64] shall apply and the following cipher suites are mandatory to support and recommended to use:

- TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487 [65].

- TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 8442 [51].

- Support of the following cipher suite is recommended:

    - TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384 as defined in RFC 8442 [51].