**3GPP TSG-SA3 Meeting #115e ad-hoc S3-241298-r1**

**Electronic meeting, online, 15 - 19 April 2024**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Updates to TLS protocol profiles**

**Document for: Approval**

**Agenda Item: 4.8**

# 1 Decision/action requested

***This pCR is to be discussed and agreed to the living document [1] for CrryptSP to TS 33.210 (v17.1.0).***

# 2 References

[1] <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_115AdHoc-e/Docs/S3-241107.zip>

# 3 Rationale

Some of the existing IETF RFC documents have been replaced by newer versions. The support of TLS1.3 to be introduced.

[ References ]

- removing replaced references

[ 6.2.1 General ]

- new RFC 9324 for best practises for TLS and DTLS referenced

- introduction of DTLS 1.3 RFC edited

[ 6.2.2 Profiling for TLS 1.3 ]

- HTTP/2 over TLS 1.3 requirements edited inclusive reference to the new edited RFC’s

[ 6.2.3 Profiling for TLS 1.2 ]

- HTTP/2 over TLS 1.2 requirements edited inclusive reference to the new edited RFC’s

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[4] Void.

[5] Void.

[6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[7] Void.

[8] Void.

[9] Void.

[10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

[11] -[25] Void.

[26] RFC‑3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec".

[27] Void.

[28] 3GPP TS 25.412: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signalling transport".

[29] Void.

[30] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; Authentication Framework".

[31] RFC-4303: "IP Encapsulating Security Payload (ESP)"

[32] Void.

[33] Void

[34] Void.

[35] RFC-4301: "Security Architecture for the Internet Protocol".

[36] Void.

[37] Void.

[38] 3GPP TS 25.422: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur interface signalling transport".

[39] 3GPP TS 25.467: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home Node B (HNB); Stage 2".

[40] 3GPP TS 25.468: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh Interface RANAP User Adaption (RUA) signalling".

[41] 3GPP TS 25.471: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iurh Interface RNSAP User Adaption (RNA) signalling".

[42] RFC-6311: "Protocol Support for High Availability of IKEv2/IPsec".

[43] RFC-7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[44] IANA: "Internet Key Exchange Version 2 (IKEv2) Parameters".

[45] Void.

[46] IETF RFC 7515: "JSON Web Signature (JWS)".

[47] IETF RFC 7516: "JSON Web Encryption (JWE)".

[48] IETF RFC 7518: "JSON Web Algorithms (JWA)".

[49] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[50] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[51] IETF RFC 8442: "ECDHE\_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2”.

[52] Void

[53] Void

[54] IETF RFC 5288: "AES Galois Counter Mode (GCM) Cipher Suites for TLS".

[55] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[56] Void.

[57] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[58] Void.

[59] Void

[60] IETF RFC 5746: "Transport Layer Security (TLS) Renegotiation Indication Extension".

[61] IETF RFC 7627: "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension".

[62] IETF RFC 7919: "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)".

[63] Void

[64] IETF RFC 5489: "ECDHE\_PSK Cipher Suites for Transport Layer Security (TLS)".

[65] IETF RFC 5487: "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode".

[66] IETF RFC 8446: “The Transport Layer Security (TLS) Protocol Version 1.3".

[67] Void

[68] Void.

[69] IETF RFC 4086: "Randomness Recommendations for Security".

[70] IETF RFC 8221: "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[71] IETF RFC 8422: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) ".

[72] IETF RFC 8937: " Randomness Improvements for Security Protocols".

[73] IETF RFC 8247: "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)".

[x1] RFC 9110: HTTP Semantics

[x2] RFC 9112: HTTP/1.1

[x3] RFC 9113: HTTP/2

[x4] RFC 9147: The Datagram Transport Layer Security (DTLS) Protocol Version 1.3

[x5] RFC 9325: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)

[x7] RFC 9525: Service Identity in TLS

[x8] RFC 7301: Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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.

NOTE1: The generic best current practice recommendations for using secure TLS and DTLS can be found in   
 RFC 9325 [x5].

NOTE2: DTLS 1.2 as specified in RFC 6347 [49] is based on TLS 1.2 and DTLS 1.3 as specified in RFC 9147 [x4] is based on TLS1.3. 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 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.

- TLS 1.3 as specified in RFC 8446 [66] shall be supported and implementations shall prefer to negotiate TLS 1.3 over earlier versions of TLS.

- If DTLS is supported then DTLS 1.2 as specified in RFC 6347 [49] shall be supported and DTLS 1.3 as specified in RFC 9147 [x4] should be supported.

**Other**

- If the TLS connection is used to transport HTTP/2 over TLS, the additional requirements specified in RFC 9113 [x3] shall be followed.

- If the TLS connection is used to transport HTTP/1.1 over TLS as specified in RFC 9112 [x2] and RFC 9110 [x1], the client shall not establish a connection "upgraded to TLS Within HTTP/1.1" per RFC 9110 [x1] and per RFC 9112 [x2], but shall only establish the tunnel over a raw TCP connection.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2.2 Profiling for TLS 1.3

For TLS 1.3 the following restrictions and extensions shall apply:

**TLS cipher suites and Diffie-Hellman groups**

- The requirements given in section 9.1 of TLS 1.3 RFC 8446 [66] and in sections 4.1, 4.3 and 4.5 of RFC 9325 [x5] shall be followed. In addition:

- Key exchange with secp384r1 should be supported.

- For HTTP/2 over TLS 1.3, the additional requirements specified in section 9.2.3 of RFC 9113 [x3] shall be followed

**TLS signature schemes**

- The general rules on TLS signatures in sections 4.1 and 4.5 of RFC 9325 [x5] shall be followed.

- ecdsa\_secp384r1\_sha384 should be supported.

**TLS extensions**

- The requirements given in sections 4.2 and 9.2 of TLS 1.3 RFC 8446 [66] and in RFC 9325 [x5] shall be followed. In addition:

- The Server Name Indication (SNI) extension defined in RFC 6066 [57] shall be supported. Also, refer to section 7.5 of RFC 9525 [x7] and sections 3.8 and 3.9 of RFC 9325 [x5] for the SNI and ALPN extensions usage with multi-server deployments (i.e., multiple presented identifiers for TLS servers).

- The Application-Layer Protocol Negotiation (ALPN) extension, defined in RFC 7301 [x8] should be supported.

- The TLS Certificate Status Request extension (i.e., for ’OCSP stapling’), as defined in RFC 6066 [57] and RFC 8446 [66] should be supported.

- For HTTP/2 over TLS 1.3, the additional requirements specified in section 9.2.3 of RFC 9113 [x3] shall be followed. Specifically, HTTP/2 servers shall not send post-handshake TLS 1.3 CertificateRequest messages and the prohibition on post-handshake authentication applies even if the client offered the ’post\_handshake\_auth’ TLS extension.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.2.3 Profiling for TLS 1.2

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

**TLS cipher suites**

- The rules on allowed cipher suites given in TLS 1.2 (RFC 5246 [50]) and in sections 4.1, 4.2 and 4.5 of RFC 9325 [x5] 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\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289 [55]

- 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 Authenticated Encryption with Associated Data (AEAD) and those offering forward secrecy (i.e., “perfect forward secrecy”, PFS)) as discussed in section 7.3 in RFC 9525 [x5] shall be supported. Additionally, as specified in section 4.1 of RFC 9325, TLS 1.2 implementations should not negotiate cipher suites based on ephemeral finite-field Diffie-Hellman key agreement (i.e., "TLS\_DHE\_\*" cipher suites).

- For HTTP/2 over TLS 1.2, the additional requirements on TLS 1.2 cipher suites specified in section 9.2.2 of RFC 9113 [x3] shall be followed. Also, the prohibited TLS 1.2 cipher suites specified in Appendix A of RFC 9113 [x3] must not be used.

**Diffie-Hellman groups**

- The general rules on Diffie-Hellman groups in sections 4.1, 4.2, 4.5 and 7.4 of RFC 9325 [x5] shall be followed.

- 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. Except curve25519, ed25519, and W-25519, elliptic curve groups of less than 256 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.

- For HTTP/2 over TLS 1.2, the additional requirements on TLS 1.2 Diffie-Hellman groups and ephemeral key exchange sizes specified in section 9.2.1 of RFC 9113 [x3] shall be followed. Also, the prohibited TLS 1.2 cipher suites specified in Appendix A of RFC 9113 [x3] must not be used.

**TLS hash algorithms and signature algorithms**

- The general rules in sections 4.1 and 4.5 of RFC 9325 [x5] shall be followed.

- 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.

- ecdsa\_secp384r1\_sha384 should be supported.

**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**

- The general rules on TLS extensions specified in sections 3 and 4.6 of RFC 9325 [x5] shall be followed.

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

- The Server Name Indication (SNI) extension defined in RFC 6066 [57] shall be supported. Also, refer to section 7.5 of RFC 9525 [x7] and sections 3.8 and 3.9 of RFC 9325 [x5] for the SNI and ALPN extensions usage with multi-server deployments (i.e., multiple presented identifiers for TLS servers).

- The Application-Layer Protocol Negotiation (ALPN) extension, defined in RFC 7301 [x8] should 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 TLS Certificate Status Request (i.e., for “OCSP stapling”), defined in RFC 6066 [57] should be supported.

- For HTTP/2 over TLS 1.2, the additional requirements on TLS 1.2 extensions and features specified in sections 9.1 and 9.2.1 of RFC 9113 [x3] shall be followed.

**PSK cipher suites**

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

- 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].

- For HTTP/2 over TLS 1.2, the additional requirements on TLS 1.2 cipher suites specified in section 9.2.2 of RFC 9113 [xx] shall be followed.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*