**3GPP TSG-SA3 Meeting #116 *S3-242413***

Jeju, South Korea, 20th - 24th May 2024 (revision of S3-241782)

**Source: Nokia, Nokia Shanghai Bell**

**Title: Updates to TLS profiles on TS33210**

**Document for: Approval**

**Agenda Item: 4.8**

# 1 Decision/action requested

***This pCR is to be approved to the living document [1] for CryptoSP to TS 33.210 (v18.0.0)***

# 2 References

[1] <https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_116_Jeju/Docs/S3-241768.zip>

# 3 Rationale

## 3.1 General

Content of the following clauses will be added to the coversheet of the living document upon approval of this document.

## 3.2 Reason for Change

IETF as well as BSI and NIST has provided updates on TLS and DTLS specific specifications.

## 3.3 Summary of change

- Minor editorial.

- Reference clause new RFC’s added.

- In clause 6.2.1 the new recommendations on TLS and DTLS added.

- In clause 6.2.2 references to updated RFC’s edited, and reference to HTTP/2 over TLS 1.3 added.

## 3.4 Consequences if not approved

Missing reference to the updated IETF specification.

# 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] IETF RFC 2817: “Upgrading to TLS Within HTTP/1.1”.

[54] Void.

[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] IETF RFC 5077: “Transport Layer Security (TLS) Session Resumption without Server-Side State”.

[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] Void.

[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)".

[XX] IETF RFC 9147: "Datagram Transport Layer Security Version 1.3".

[YY] IETF RFC 9110: "HTTP Semantics".

[XZ] IETF RFC 8750: "Implicit Initialization Vector (IV) for Counter-Based Ciphers in Encapsulating Security Payload (ESP)”

[x1] RFC 9110: HTTP Semantics

[x2] RFC 9112: HTTP/1.1

[x3] IETF RFC 9113: “HTTP/2”.

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

## \*\*\*\*\*\*\* End of 1st 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.

NOTE 1: Recommendations for Secure Use of TLS and DTLS can be found in RFC 9325 [x5] and RFC 9113 [x3].

NOTE2: DTLS 1.2 as specified in RFC 6347 [49] is based on TLS 1.2. DTLS 1.3 as specified in RFC 9147 [XX] is based on TLS 1.3. 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 and DTLS 1.3 as specified in RFC 9147 [XX] should be supported.

- 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, then the additional requirements specified in RFC 9113 [x3] shall be followed.- If the TLS connection is used for the https URI Scheme as specified in RFC 9110 [YY], then 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.

## \*\*\*\*\*\*\* Start of 2nd 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] shall be followed. In addition:

- Key exchange with secp384r1 should be supported.

- Ffdhe2048 shall not be supported.

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

**TLS signature schemes**

- ecdsa\_secp384r1\_sha384 should be supported.

**TLS PSK key exchange modes**

- psk\_ke shall not be supported.

**TLS cipher suites**

- TLS\_SHA256\_SHA256 and TLS\_SHA384\_SHA384 shall not 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 TLS Certificate Status Request extension (i.e., "OCSP stapling"), as defined in RFC 6066 [57] and RFC 8446 [66] should be supported.

- For HTTP/2 over TLS 1.3, then 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 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*