**3GPP TSG-SA3 Meeting #116 *S3-242664***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **draftCR** | **rev** |  | **Current version:** | **18.0.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for CryptoSP: draftCR to TS 33.210, Updates to cryprographic profiles | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | CryptoSP | | | | |  | ***Date:*** | | | 2024-05-05 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***Release:*** | | | Rel-19 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | - As stated in RFC 9206 and NIST SP 800-56A there are security concerns with reuse of Diffie-Hellman private keys.  - AES-CBC was removed as mandatory to implement in Rel-15. AES-CBC was intended to be used with HMAC-SHA256. Mandatory support of AUTH\_HMAC\_SHA256\_128 is not necessary anymore. Note that confidentiality is mandatory in IKEv2 but optional in ESP. - RFC 9206 clarifies that Identification Payloads must not be used for authentication.  - IETF has published DTLS 1.3. DTLS 1.2 is now obsolete. When TLS 1.3 was published, 3GPP quickly mandated TLS 1.3. The security reasons to use DTLS 1.3 is equally strong as those to use TLS 1.3. NIST mandates TLS 1.3 since Jan 2024, also in already deployed nodes. However there are not many libraries supporting DTLS 1.3 and DTLS/SCTP cannot be used with DTLS 1.3. We therefore only suggest that DTLS 1.3 should be supported but not mandated.  **From SA3#115Adhoc-e:**  - IETF has published QUIC and 3GPP Rel-18 is using QUIC. Both DTLS 1.3 and QUIC use the TLS 1.3 handshake.  - IETF is planning to deprecate all use of Diffie Hellman over a finite field (DHE) in TLS 1.2. (3GPP already forbids support of non-ephemeral DH) [<https://datatracker.ietf.org/doc/draft-ietf-tls-deprecate-obsolete-kex/>].  - IETF is planning to mark the TLS 1.3 cipher suites TLS\_SHA256\_SHA256 and TLS\_SHA384\_SHA384 as Discouraged (D) [<https://www.ietf.org/archive/id/draft-ietf-tls-rfc8447bis-08.html>].  - RFC 2818 has been obsoleted by RFC 9110.4  - According to the guidelines in [<https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf>] by BSI, ffdhe2048 can only be used up to 2022 and psk\_ke only up to 2026. Some TLS 1.3 libraries do not support ffdhe2048 and psk\_ke due to the inadequate security. Thus, ffdhe2048 shall not be supported.  - CTR, CCM, GCM, GMAC, and ChaCha20-Poly1305 in ESP are not designed for use with random IVs and IETF requires that the 64-bit IVs are unique. NIST SP 800-38D [<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>] specifying AES-GCM and AES-GMAC requires that the length of the random field in the GCM nonce shall be at least 96 bits. While revising SP 800-38D, NIST finds [<https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/decision-proposal-comments/sp800-38d-decision-proposal-comments-2023.pdf>] that GCM with a 96-bit random nonces gives less than 97 bits of security.  - Currently, GCM, GMAC, CTR, CCM, and ChaCha20-Poly1305 in ESP uses an explicit 64-bit IV. The 8-byte IV MUST NOT repeat for a given key, which means that the IV must be a counter or the output of an LFSR. Random 64-bit IVs are also forbidden by NIST, which requires in 800-38D that the length of the random field in the GCM nonce shall be at least 96 bits.  **From SA3#116:**   * IETF as well as BSI and NIST has provided updates on TLS and DTLS specific specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | - Mandatory support of AUTH\_HMAC\_SHA256\_128 is removed.  - Reuse of Diffie-Hellman private keys is forbidden. - Clarification that Identification Payloads must not be used for authentication.  - DTLS 1.3 should be supported.  The changes are (i) Adding text clarifying that it is not allowed to use random 64-bit IVs (ii) clarifying that constructing the IV in CBC from the encrypted data is no longer common and corrected some editorials.  **From SA3#115Adhoc-e:**  - Clarify that the 3GPP TLS profile also applies to QUIC.  - Support of FFDH in TLS 1.2 is forbidden. Mandatory to support cipher suites are updated based on this. Reference [54] is voided.  - TLS\_SHA256\_SHA256 and TLS\_SHA384\_SHA384 are forbidden to support.  - ffdhe2048 and psk\_ke are forbidden to support.  - RFC 2818 is voided and replaced with RFC 9110.  - The proposed change is to add text stating that initiators should propose implicit IV (IIV) algorithms.  **From SA3#116:**  - 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. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | - Implementations might reuse Diffie-Hellman private keys which has security concerns.  - Inconsistent profile as AUTH\_HMAC\_SHA256\_128 without a legacy non-AEAD encryption algorithm. - Implementations might use Identification Payloads for “authentication”, i.e., there is not authentication.  **From SA3#115Adhoc-e:**  - Misalignment with IETF and BSI Specs. Weak and non-recommended security algorithms keep being used.  - If these changes are not Approved, some vendors might use 64-bit random IVs in ESP, which is not secure and forbidden by IETF and NIST.  - If not approved, it may cause worse performance.  **From SA3#116:**   * Missing reference to the updated IETF specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.3.3, 5.3.5, 5.4.2, 6.2.1, 6.2.2, 6.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | SA3#115: S3-240877, S3-240878  SA3#115Adhoc-e: S3-241521, S3-241633, S3-241278,S3-241279  SA3#116: S3-242417, S3-242413 | | | | | | | | |

## \*\*\*\*\*\*\* FIRST 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)".

[x] RFC 9110: "HTTP Semantics".

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

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

[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)”.

## \*\*\*\*\*\* NEXT CHANGE **\*\*\*\***

### 5.3.3 Support of ESP encryption transforms

The implementation conformance requirements for ESP encryption transforms (including authenticated encryption transforms) in RFC 8221 [69] shall be followed.

Only the ESP encryption algorithms (including authenticated encryption algorithms) mentioned in RFC 8221 [70] or RFC 8750 [XZ] shall be used. Algorithms marked with "MUST" shall be supported. Initiators should propose implicit IV variant of algorithms as defined in RFC 8750 [XZ], while negotiating the ESP encryption transforms, as they have higher performance.

## \*\*\*\*\*\*\* Next CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.3.5 Requirements on the construction of the IV

The following strengthening of the requirements on how to construct the IV shall take precedence over the description given in RFC‑2451 [24] section 3 and all other descriptions that allow for predictable IVs.

- For CBC mode: the IV field shall be the same size as the block size of the cipher algorithm being used. The IV shall be chosen at random, and shall be unpredictable to any party other than the originator.

- For CTR, GCM, CCM, ChaCha20-Poly1305 and GMAC mode: the IV field is 8 octets. The IV shall be generated in a manner that ensures uniqueness. The same IV and key combination shall not be used more than once. - It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process. It is explicitly not allowed to use a random IV.

The previously common practice of constructing an IV in CBC mode from the encrypted data of the preceding encryption process means that the IV is disclosed before it is used. A predictable IV exposes IPsec to certain attacks irrespective of the strength of the underlying cipher algorithm. The first bullet point forbids this practice in the context of NDS/IP.

These requirements on CBC mode imply that the network elements shall have a capability to generate random data. RFC 4086 [69] gives guidelines for hardware and software pseudorandom number generators.

## \*\*\*\*\*\*\* Next CHANGE \*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.4.2 Profiling of IKEv2

The Internet Key Exchange protocol IKEv2 shall be supported for negotiation of IPsec SAs. The following additional requirements apply.

**General:**

IKEv2 Configuration Payload as defined in RFC 7296 [43] should be supported.

Protocol support for High Availability as defined in RFC 6311 [42] should be supported.

An ephemeral private key shall be used in exactly one key establishment transaction and shall be destroyed (zeroized) as soon as possible.

**For IKE\_SA\_INIT exchange:**

The following algorithms are listed with their names according to [44].

Following algorithms shall be supported:

- Confidentiality: AES-GCM with a 16 octet ICV with 128-bit key length;

- Pseudo-random function: PRF\_HMAC\_SHA2\_256;

- Diffie-Hellman group 19 (256-bit random ECP group) ;

Following algorithms should be supported:

- Confidentiality: AES-GCM with a 16 octet ICV with 256-bit key length;

- Pseudo-random function: PRF\_HMAC\_SHA2\_384;

- Diffie-Hellman group 20 (384-bit random ECP group).

- Diffie-Hellman group 31 (Curve25519).

NOTE 1: The IANA IKEv2 registry [44] contains further references for the algorithms listed.

For security reasons, the use of Diffie-Hellman MODP groups less than 2048-bit shall not be supported.

**For IKE\_AUTH exchange:**

- Authentication method 2 - Shared Key Message Integrity Code shall be supported;

- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;

- Re-keying of IPsec SAs and IKE SAs shall be supported as specified in RFC 7296 [43].

- In addition to the requirements defined in RFC 7296 [43], rekeying shall not lead to a noticeable degradation of service.

- Identification Payloads (IDi and IDr) shall not be used for the IKEv2 authentication but may be used for policy lookup.

**For the CREATE\_CHILD\_SA exchange:**

- A DH key exchange should be used (giving Perfect Forward Secrecy) and the session keys should be changed frequently.

**For reauthentication:**

- Reauthentication of IKE SAs as specified in RFC 7296 [43] section 2.8.3 shall be supported;

- A NE shall proactively initiate reauthentication of IKE SAs, and creation of its Child SAs, i.e. the new SAs shall be established before the old ones expire;

- A NE shall destroy an IKE SA and its Child SAs when the authentication lifetime of the IKE SA expires;

NOTE 2: NE actions related to reauthentication are controlled by locally configured lifetimes according to RFC 4301 [35]: a soft authentication lifetime that warns the implementation to initiate reauthentication, and a hard authentication lifetime when the current IKE SA and its Child SAs are destroyed.

- In addition to the requirements defined in RFC 7296 [43], reauthentication shall not lead to a noticeable degradation of service.

## \*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\*

## \*\*\*\*\*\*\* NEXT CHANGE \*\*\*\*\*\*\*\*\*\*\*\*

## 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 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.

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

## 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.

## 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]

- 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 AEAD (e.g. GCM) and PFS (i.e., ECDHE) 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. Except x25519, elliptic curve groups of less than 256 bits shall not be supported.

- Finite field Diffie-Hellman (i.e. DHE) 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.

- 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**

- 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) extension, defined in RFC 6066 [57] should be supported.

**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].

## \*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\*