**3GPP TSG-SA3 Meeting #115 *S3-240876***

Athens, Greece, 26th February - 1st March 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** | **draftCR** | **rev** |  | **Current version:** | **17.1.0** |  |
|  |
| *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:***  | Draft CR on CryptoSP TS 33.210 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | CryptoSP |  | ***Date:*** | 2024-03-01 |
|  |  |  |  |  |
| ***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 canbe 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. |
|  |  |
| ***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. |
|  |  |
| ***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. |
|  |  |
| ***Clauses affected:*** | 5.4.2, 6.2 |
|  |  |
|  | **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 |

## \*\*\*\*\*\*\* First 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: 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 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 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 signature schemes**

- ecdsa\_secp384r1\_sha384 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 extension (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]

- 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 (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. 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.

**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\_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].

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