**3GPP TSG-SA3 Meeting #115 *S3-240877-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **0079** | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HELP***](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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Updates to the IKEv2 profile | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | CryptoSP | | | | |  | ***Date:*** | | | 2024-02-19 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***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:*** | | - 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. - BSI TR-02102-3 states that 2048-bit MODP group is only for use up until 2022. NIST and ANSSI only allow 2048-bit Finite Field Diffie-Hellman if the data does not have to be protected after 2030.The is no reason to support or use 2048-bit MODP as the strong Diffie-Hellman group 19 has been mandatory to support since Rel-13.  - As stated in RFC 9206 and NIST SP 800-56A there are security concerns with reuse of Diffie-Hellman private keys. - RFC 9206 clarifies that Identification Payloads must not be used for authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | - Mandatory support of AUTH\_HMAC\_SHA256\_128 is removed. - Support of 2048-bit MODP Groups is forbidden.  - Reuse of Diffie-Hellman private keys is forbidden. - Clarification that Identification Payloads must not be used for authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | - Inconsistent profile as AUTH\_HMAC\_SHA256\_128 without a legacy non-AEAD encryption algorithm. - The weak 2048-bit MODP Groups might be used in violation with BSI recommendations. - Implementations might reuse Diffie-Hellman private keys which has security concerns. - Implementations might use Identification Payloads for “authentication”, i.e., there is not authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

## \*\*\*\*\*\*\* 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 \*\*\*\*\*\*\*\*\*\*\*\*