**3GPP TSG-SA3 Meeting # 108-e *S3-222048-r1***

**e-meeting, 22 -**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.210** | **CR** | **074** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCryptPr | | | | |  | ***Date:*** | | | 2022-08-26 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The latest version, RFC 8247 is an update over RFC 7296., is an upgrade to IKEV2 RFC 7296. IPsec RFC references from RFC 7296(IKEv2) to RFC 8247. It is a fairly mundane update of pointing the references to the latest IETF specs and honoring the latest recommendations on the algorithmic suggestions, which include sunsetting some of the older algorithms such as MODP1024s160, MODP768, PRF-MD5, HMAC-MD5 etc Rfc8237 prohibits the use of MD5 and change s the requirement of 3DES-CBC from optional from mandatory. MD5 has been deprecated by NIST and is no longer mentioned in publications such as [NISTSP800-131A-R2]. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | CR proposes following  1) Replace IKEv2 rfc 7296 with rfc 8247. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Obsolete algorithms persists in implementation | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 5.2.0, | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

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] Void.

[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] IETF RFC 2818: "HTTP Over TLS".

[53] IETF RFC 2817: "Upgrading to TLS Within HTTP/1.1".

[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] 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] 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".

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

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

5.2 Security Associations (SAs)

5.2.0 General

For NDS/IP-networks the key management and distribution between SEGs is handled by the protocol Internet Key Exchange Internet Key Exchange (IKEv2) (RFC 8247 [ZZ]). The main purpose of IKEv2 is to negotiate, establish and maintain Security Associations between parties that are to establish secure connections. The concept of a Security Association is central to IPsec and IKEv2.

To secure a typical, bi-directional communication between two nodes using IKEv2 an IKE SA is established through which the Child Security associations i.e. IPsec security associations are established.

IPsec Security associations are uniquely defined by the following parameters:

- A Security Parameter Index (SPI);

- An IP Destination Address (this is the address of the ESP SA endpoint);

- A security protocol identifier (this will always be the ESP protocol in NDS/IP).

With regard to the use of IPsec security associations in the network domain control plane of NDS/IP-networks the following is noted:

- NDS/IP only requires support for ESP SAs;

The specification of IPsec SAs can be found in RFC4301 [35].

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

5.4.0 General

NOTE:

Clause 5.4 contains the general 3GPP IKEv2 profile. Other 3GPP specifications point to clause 5.4. Thus parts of clause 5.4 may also apply to devices and network nodes as specified in other specifications. New specifications using IKE should refer to this profile with as few exceptions as possible. Unless explicitly stated otherwise, the 3GPP IKEv2 profile apply for all uses of IKEv2 to protect 3GPP interfaces.

NOTE: Clause 6.2.1b of TS 33.310 [30] provides additional requirements to the general 3GPP IKEv2 profile when certificate based IKEv2 authentication is used.

5.4.1 Void

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 8247 [ZZ] should be supported.

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

**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;

- Integrity: AUTH\_HMAC\_SHA256\_128;

- 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 8247 [ZZ].

- In addition to the requirements defined in RFC 8247 [ZZ], rekeying shall not lead to a noticeable degradation of service.

**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 8247 [ZZ] 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 8247 [ZZ], reauthentication shall not lead to a noticeable degradation of service.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

## 5.6 Network domain security key management and distribution architecture for native IP based protocols

### 5.6.1 Network domain security architecture outline

The NDS/IP key management and distribution architecture is based on the IKEv2 (RFC 8247 [ZZ]) protocol. As described in the previous section a number of options available in the full IETF IPsec protocol suite have been considered to be unnecessary for NDS/IP. Furthermore, some features that are optional in IETF IPsec have been mandated for NDS/IP and lastly a few required features in IETF IPsec have been deprecated for use within NDS/IP scope. Sections 5.3 and 5.4 give an overview over the profiling of IPsec and IKEv2 in NDS/IP.

The compound effect of the design choices in how IPsec is utilized within the NDS/IP scope is that the NDS/IP key management and distribution architecture is quite simple and straightforward.

The basic idea to the NDS/IP architecture is to provide hop-by-hop security. This is in accordance with the *chained-tunnels* or *hub-and-spoke* models of operation. The use of hop-by-hop security also makes it easy to operate separate security policies internally and towards other external security domains.

In NDS/IP only the Security Gateways (SEGs) shall engage in direct communication with entities in other security domains for NDS/IP traffic. The SEGs will then establish and maintain IPsec secured ESP Security Association in tunnel mode between security domains. SEGs will normally maintain at least one IPsec tunnel available at all times to a particular peer SEG. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs may be able to establish and maintain ESP Security Associations as needed towards a SEG or other NEs within the same security domain. All NDS/IP traffic from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will be afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP Security Association between two communicating security domains. This would make for coarse-grained security granularity. The benefits to this is that it gives a certain amount of protection against traffic flow analysis while the drawback is that one will not be able to differentiate the security protection given between the communicating entities. This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.



Figure 1: NDS architecture for IP-based protocols

Additional guidelines on how to apply IPsec in SCTP are specified in RFC3554 [26]. This RFC is optional for implementation unless otherwise explicitly indicated per reference point.

NOTE: TS 33.310 [30] defines an inter-operator Public Key Infrastructure (PKI) that can be used to support the establishment of IPsec connections.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***