**3GPP TSG-SA3 Meeting #104-e *draft\_*S3-213023-r1**

**e-meeting, 16th - 29th May 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **Draft** | **rev** |  | **Current version:** |  |  |
|  |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Security updates for algorithms and protocols in 33.210 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eCryptPr |  | ***Date:*** | 2021-05-10 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** |  |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | - Duplicate text in clause 1.- Reference to TLS 1.1 and RFC 4279 cipher suites which are forbidden to support.- References to voided [12] and [17]. Several places mention IKEv1 which was removed many releases ago.- In Rel-16 3GPP added a recommendation on frequent use of DH key exchange. ANSSI recommends rekeying at least every hour. With frequent rekeying it becomes more important with low latency DH key exchange.- Several 3GPP document has forgotten to add references to the general 3GPP security profiles for TLS and IPsec. This opens up the risk that TLS 1.0 , RC4, DES is used in practice.- Several 3GPP document using TLS forgot to add a reference to the one of the 3GPP certificate profiles. This opens up the risk that SHA-1 or RSA-512 is used in practice.- The text about the IKEv2 and ESP profiles are notes while the text about the TLS profile is not. This is inconsistant.- Easy to miss that part of the 3GPP IKEv2 profile is in TS 33.310- Text about IV creating in ESP talks about avoiding predictability in GCM and CTR which is wrong.- IETF has published more guidelines on randomness complementing RFC 4086. |
|  |  |
| ***Summary of change:*** | - Duplicate text removed.- References to TLS 1.1 and RFC 4279 are voided.- Text referencing [12] is [17] is not needed and is removed. Text mentioning IKEv1 is removed. Annex E is voided.- The Diffie-Hellman group 31 (Curve25519) is added as should support for IKEv2. Curve25519 is already mandatory to support for SUCI and is should support for TLS.- Change so that the general text about the security profiles are not notes. Added that the profiles apply unless otherwise stated. Added that the TLS cerficate profiles apply unless otherwise stated.- Added a note in the IKEv2 profilign refering the the other part of the profile in TS 33.310.- Separated guidance on IV creation for CBC and GCM and added a reference to RFC 8037. |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 1, 2, 3.1, 4.2, 5.3, 5.4, 6.2.1, 6.2.3, Annex A.2, Annex E |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN CHANGES \*\*\*

# 1 Scope

The present document defines the security architecture for network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks. . The present document furthermore serves as a central repository for cryptographic profiles for security above IP layer.

\*\*\* NEXT 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] 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) ".

[Z1] IETF RFC 8937: " Randomness Improvements for Security Protocols".

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

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [2].

**Anti-replay protection:** Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographical integrity mechanism in place.

**Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

**Data integrity:** The property that data has not been altered in an unauthorised manner.

**Data origin authentication:** The corroboration that the source of data received is as claimed.

**Entity authentication:** The provision of assurance of the claimed identity of an entity.

**Key freshness:** A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

**NDS/IP Traffic:** Traffic that requires protection according to the mechanisms defined in this specification.

**NDS/IP-networks:** 3GPP and fixed broadband networks.

**IPsec Security Association:** A unidirectional logical connection created for security purposes. All traffic traversing a SA is provided the same security protection. The SA itself is a set of parameters to define security protection between two entities. A IPsec Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

**Security Domain**: Networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical.

**Transit Security Domain:** A security domain, which is transmitting NDS/IP traffic between other security domains.

**Transport mode**: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers.

**Tunnel mode**: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected.

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

##  4.2 Protection at the network layer

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC-4301 [35].

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

## 5.3 Profiling of IPsec

### 5.3.0 General

This section gives an overview of the features of IPsec that are used by NDS/IP. The overview given here defines a minimum set of features that shall be supported. In particular, this minimum set of features is required for interworking purposes and constitutes a well-defined set of simplifications.

The accumulated effect of the simplifications is quite significant in terms of reduced complexity. This is achieved without sacrificing security in any way. It shall be noted explicitly that the simplifications are specified for NDS/IP and that they may not necessarily be valid for other network constellations and usages.

Within their own network, operators are free to use IPsec features not described in this section although there should be no security or functional reason to do so.

Clause 5.3 contains the general 3GPP IPsec ESP profile. Other 3GPP specifications (e.g. TS 33.203 [10], etc.) may point to clause 5.3. Thus parts of clause 5.3 may also apply to devices and network nodes as specified in other specifications. New specifications using ESP should refer to this profile with as few exceptions as possible. Unless explicitly stated otherwise, the 3GPP ESP profile apply for all uses of ESP to protect 3GPP interfaces.

### 5.3.1 Support of ESP

When NDS/IP is applied, the ESP security protocol shall be used. IPsec ESP shall be supported according to RFC-4303 [31]. Extended sequence number may be supported.

### 5.3.2 Support of tunnel mode

Since security gateways are an integral part of the NDS/IP architecture, tunnel mode shall be supported. For NDS/IP inter-domain communication, security gateways shall be used and consequently only tunnel mode (RFC-4301 [35]]) is applicable for this case.

### 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] shall be used. Algorithms marked with "MUST" shall be supported.

### 5.3.4 Support of ESP authentication transforms

The implementation conformance requirements for ESP authentication transforms in RFC 8221 [70] shall be followed.

Only the ESP authentication algorithms mentioned in RFC 8221 [70] shall be used. Algorithms marked with "MUST" shall be supported. AES-GMAC with AES-128 shall be supported.

ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the NULL authentication algorithm is explicitly not allowed for use, unless an authenticated encryption algorithm is used.

### 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, and GMAC mode: the IV field shall be 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.

The common practice of constructing the IV 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 second bullet point forbids this practice in the context of NDS/IP.

These requirements 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 \*\*\*

### 5.4.0 General

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 7296 [43] 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 7296 [43].

- In addition to the requirements defined in RFC 7296 [43], 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 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.

### 5.4.3 Void

\*\*\* NEXT 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: 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.

**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.

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

## 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]

- 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].

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

# A.2 Filtering routers and firewalls

In order to strengthen the security for IP based networks, border gateways and access routers would normally use packet filtering strategies to prevent certain types of traffic to pass in or out of the network. Similarly, firewalls are used as an additional measure to prevent certain types of accesses towards the network.

The rationale behind the application of packet filters and firewalls could be found in the security policy of the network operator. Preferably, the security policy would be an integral part of the network management strategy as a whole.

While network operators are strongly encouraged to use filtering routers and firewalls, the usage, implementation and security policies associated with these are considered outside the scope of this document.

Simple filtering may be needed before the Security Gateway (SEG) functionality. The filtering policy allosw key protocols such as DNS and NTP to pass. This will include traffic over the Za interface from IKEv2 and IPsec ESP in tunnel mode. Unsolicited traffic is rejected.

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

Annex E:
Void.

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