**3GPP TSG-SA3 Meeting # 108-e *S3-222047***

 **e-meeting,** 22 **- 26 August 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.210** | **CR** | **0073** | **rev** | **-** | **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:***  | Update IPSec references to rfc8221 |
|  |  |
| ***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 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | RFC 8221 has the following verbiage change from using deprecated MD5, SHA1, and DES-CBS algorithms. Rfc8221 prohibits the use of MD5 and changes 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]. NIST formally deprecated the use of SHA-1 in 2011 [NISTSP800-131A-R2] and disallowed its use for digital signatures at the end of 2013, based on both the Wang et. al; attack and the potential for a brute-force attack. (<https://csrc.nist.gov/CSRC/media/Publications/sp/800-131a/rev-2/draft/documents/sp800-131Ar2-draft.pdf>). Also, according to draft guidance published by NIST on July 19, 2018, the Triple Data Encryption Algorithm (TDEA or 3DES) is officially being retired. The guidelines propose that 3DES is deprecated for all new applications after a period of public consultation and usage is disallowed after 2023. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf> |
|  |  |
| ***Summary of change:*** | CR proposes following 1) Algorithm implemetion and Usage guidence should follow the latest rfc 8221 for ESP |
|  |  |
| ***Consequences if not approved:*** | Obsolete algorithms persists in implementation  |
|  |  |
| ***Clauses affected:*** | 2, 5.3.1 |
|  |  |
|  | **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".

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

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.

NOTE: Void

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. Usage guidance for the Implementation of Cryptographic Algorithm for ESP shall follow RFC-8221[70].

NOTE: Void

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