**3GPP TSG-SA3 Meeting #107-e *S3-220643-r1***

**e-meeting, 16 - 20 May 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.203** | **CR** | 0265 | **rev** | 1 | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Modernization of the Integrity & Encryption Algorithms between UE and P-CSFC |
|  |  |
| ***Source to WG:*** | Deutsche Telekom AG |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-04-19 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | TS 32.203 describes that "Hmac-sha-1-96" and "aes-cbc" are not recommended. But it does not show any improvements which agorithms sould be used. To increase security this CR proposes to add the SAH2 algorithms 128 and 512\_256 according to RFC 6234.This algorithms are state of the art and recomenden by national security agencies like NIST in US or BSI in Germany.Also the addition of an encrypt-algorithm “chacha20\_poly1305” is proposed according to RFC 8439  |
|  |  |
| ***Summary of change:*** | Add SAH2 algorithms according to RFC 6234 |
|  |  |
| ***Consequences if not approved:*** | Security requirements according to national security agencies canot be aplied. |
|  |  |
| ***Clauses affected:*** | Annex H |
|  |  |
|  | **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:*** |  |

\*\*\* BEGINNING OF CHANGES \*\*\*

Annex H (normative):
The use of "Security Mechanism Agreement for SIP Sessions" [21] for security mode set-up

The BNF syntax of RFC 3329 [21] is defined for negotiating security associations for semi-manually keyed IPsec or TLS in the following way:

 security-client = "Security-Client" HCOLON sec-mechanism \*(COMMA sec-mechanism)

 security-server = "Security-Server" HCOLON sec-mechanism \*(COMMA sec-mechanism)

 security-verify = "Security-Verify" HCOLON sec-mechanism \*(COMMA sec-mechanism)

 sec-mechanism = mechanism-name \*(SEMI mech-parameters)

 mechanism-name = "ipsec-3gpp" / "tls"

 mech-parameters = ( preference / algorithm / protocol / mode / encrypt-algorithm / spi‑c / spi‑s / port‑c / port‑s )

 preference = "q" EQUAL qvalue

 qvalue = ( "0" [ "." 0\*3DIGIT ] ) / ( "1" [ "." 0\*3("0") ] )

 algorithm = "alg" EQUAL ("hmac-sha-1-96" / "hmac\_sha2\_256\_128" /
 "hmac\_sha2\_512\_256" / "aes-gmac" / "null" )

 protocol = "prot" EQUAL ( "ah" / "esp" )

 mode = "mod" EQUAL ( "trans" / "tun" / "UDP-enc-tun" )

 encrypt-algorithm = "ealg" EQUAL ("aes-cbc" / "aes-gcm" / "chacha20\_poly1305" / "null" )

 spi‑c = "spi‑c" EQUAL spivalue

 spi‑s = "spi‑s" EQUAL spivalue

 spivalue = 10DIGIT; 0 to 4294967295

 port‑c = "port‑c" EQUAL port

 port‑s = "port‑s" EQUAL port

 port = 1\*DIGIT

The changes compared to RFC 3329 [21] are:

 "alg" parameter: Addition of "aes-gmac", "hmac\_sha2\_256\_128" and "hmac\_sha2\_512\_256" and "null".
 Removal of "hmac-md5-96"

 "ealg" parameter: Addition of "aes-cbc", "chacha20\_poly1305" and "aes-gcm". Removal of "des-ede3-cbc"

 "mod" parameter: Addition of "UDP-enc-tun"

"Hmac-sha-1-96" and "aes-cbc" are not recommended.

The use of security association parameters is specified in clauses 7.1, 7.2, M.7.1 and M.7.2 of the present document. The parameters described by the BNF above have the following semantics:

 Mechanism-name: For manually keyed IPsec, this field includes the value "ipsec-3gpp". "ipsec‑3gpp" mechanism extends the general negotiation procedure of RFC 3329 [21] in the following way:

1 The server shall store the Security-Client header received in the request before sending the response with the Security-Server header.

2 The client shall include the Security-Client header in the first protected request. In other words, the first protected request shall include both Security-Verify and Security-Client header fields.

3 The server shall check that the content of Security-Client headers received in previous steps (1 and 2) are the same.

Mech-parameters: Of the mech-parameters, only preference is relevant when the mechanism-name has the value "tls".

 Preference: As defined in RFC 3329 [21].

 Algorithm: Defines the authentication algorithm. The algorithm parameter is mandatory. The value "aes-gmac" refers to the authentication algorithm ENCR\_NULL\_AUTH\_AES\_GMAC defined in IETF RFC 4543 [74]. The value "null" shall only be used with encryption algorithm "aes-gcm".

 Protocol: Defines the IPsec protocol. May have a value "ah" or "esp". If no Protocol parameter is present, the value will be "esp".

NOTE 1: According to clause 6 only "esp" (RFC 4303 [54]) is allowed for use in IMS.

 Mode: Defines the mode in which the IPsec protocol is used. May have a value "trans" for transport mode, and value "tun" for tunneling mode. If no Mode parameter is present, the value will be "trans".

NOTE 2: Void.

 Encrypt-algorithm: If present, defines the encryption algorithm. The value "aes-cbc" refers to the algorithm defined in IETF RFC 3602 [22]. The value "aes-gcm" refers to the encryption algorithm AES-GCM with a 16 octet ICV defined in IETF RFC 4106 [73]. If no Encrypt-algorithm parameter is present, the algorithm will be "null". The value "aes-gcm" shall only be used with authentication algorithm equal to "null".

 Spi‑c: Defines the SPI number of the inbound SA at the protected client port.

 Spi‑s: Defines the SPI number of the inbound SA at the protected server port.

 Port‑c: Defines the protected client port.

 Port‑s: Defines the protected server port.

It is assumed that the underlying IPsec implementation supports selectors that allow all transport protocols supported by SIP to be protected with a single SA.

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