**3GPP TSG-SA3 Meeting #105-e *S3-214307-r1***

e-meeting, 8 - 19 November 2021

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.203** | **CR** | **0262** | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  |
| *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 | **X** | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Security updates for algorithms and protocols in 33.203 |
| ***3*** |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eCryptPr |  | ***Date:*** | 2021-11-01 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | This document is a resubmission of S3-212065 and S3-213021 with the overlap with S3-214055 removed.- 3GPP should not rely on obsolete standards. This is especially true for security standards:* ICE, STUN, TURN (RFC 5245 [59], RFC 5389 [69], RFC 5766 [61]) mandates use of SHA-1. They have been obsoleted by RFC 8445, RFC 8839, RFC 8489, and RFC 8656 which mandates support of SHA-256.
* IPv6 privacy (RFC 3041 [18]) mandates use of MD5. It has been obsoleted by RFC 8981 which mandates support of SHA-256.

- No reference to TS 33.401 [55]- RFC 2817 should be [63] not [62]- Annex H and I specify use of SHA-1. As GMAC has been mandatory to support since Rel-13. SHA-1 can be removed. Without SHA-1 there is no need for CBC mode.- Annex S (Intra-domain Domain Security) mandates support of IKEv1, SHA-1, 3DES, and MD5. IKEv1 (RFC 2407 [47], RFC 2408 [48], RFC 2409 [49]) has been obsoleted by IKEv2 (RFC 7296). IKEv1 has not been allowed in 3GPP since Rel-11.- Annex O (TLS based access security) mandates the 3GPP profile but talks about TLS 1.0, TLS 1.1 and NULL cipher suites, which are all forbidden by the 3GPP TLS profile.- IMS authentication in 3G, 4G, and 5G uses “AKAv1-MD5” which has several significant security weaknesses:* MD5 is much weaker than the weak SHA-1 algorithm and should be phased-out and long-term be forbidden to use everywhere, especially in critical infrastructure like 5G.
* AKAv1 is vulnerable to "man-in-the-middle" attacks.
* AKAv2-SHA-256 addresses both problems and is already used in other parts of TS 33.203.

VoLTE and VoNR are essntial 5G mechanisms based on IMS. MD5, SHA-1, 3DES, TLS 1.0, TLS 1.1, are very algorithms that may offer a false sense of security. They should not be used in any system, especially not critical infrastructure. Critical 3GPP infrastructure like 5G should use only use recommended best practice algorithms. |
|  |  |
| ***Summary of change:*** | - ICE (RFC 5245 [59]), STUN (RFC 5389 [69]), and TURN (RFC 5766 [61]) are voided and replaced with RFC 8445, RFC 8839, RFC 8489, and RFC 8656.- IPv6 privacy (RFC 3041 [18]) is voided and replaced with RFC 8981.- TS 33.401 [55] is voided.- Reference to RFC 2817 is changed from [62] not [63]- SHA-1 and CBC is removed from Annex H and I.- IKEv1, SHA-1, 3DES, and MD5 are removed from Annex S and replaced with the 3GPP IKEv2 and ESP profiles.- TLS 1.0, TLS 1.1, and NULL are removed from Annex O.- AKAv2-SHA-256 is introduced as mandatory to support. AKAv1-MD5 is still supported to maintain backwards compatibility with pre Rel-17 releases. |
|  |  |
| ***Consequences if not approved:*** | - MD5, SHA-1, 3DES, TLS 1.0, TLS 1.1, are very algorithms that may offer a false sense of security. They should not be used in any system, especially not critical infrastructure.- Referencing obsolete RFCs makes 3GPP 5G standards look old. There is also a security risk as obsolete RFCs often have obsolete security and privacy guidelines.- Implementors might believe that support of TLS 1.0 and 1.1 are mandatory to support.- IMS, VoLTE, and VoNR continue to rely on the very weak AKAv1-MD5 algorithm. |
|  |  |
| ***Clauses affected:*** | 2, 6.1.1, 7.5, Annex H, Annex I, Annex O.2.1, Annex S.5.3, Annex S.5.4.2.1, Annex S.5.4.2.2, Annex W.3.1.2, Annex W.3.1.3, Annex W.3.3, Annex X.2.2.3, Annex X.5.1, Annex X.5.2 |
|  |  |
|  | **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:*** |  |

\*\*\* BEGIN 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] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[2] Void.

[3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".

[4] Void.

[5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[6] IETF RFC 3261 "SIP: Session Initiation Protocol".

[7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".

[8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".

[9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".

[10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".

[11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".

[12] Void.

[13]-[16] Void.

[17] IETF RFC 3310 (2002): "HTTP Digest Authentication Using AKA". April, 2002.

[18] Void.

[19] Void.

[20] Void.

[21] IETF RFC 3329 (2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[22] Void.

[23] IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[24] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[25] Void.

[26] ETSI ES 282 001: "TISPAN - Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture for NGN Release 1".

[27] IETF RFC 3947 (2005): "Negotiation of NAT-Traversal in the IKE".

[28] IETF RFC 3948 (2005): "UDP Encapsulation of IPsec ESP Packets".

[29] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[30] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

[31] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions”.

[32] IETF RFC 5626 (2009): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

[33] Void.

[34] Void.

[35] Void.

[36] ETSI ES 282 004: “NGN Functional Architecture; Network Attachment Sub-System (NASS)”

[37] ETSI TS 187 001: " Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements"

[38] Void.

[39] 3GPP TS 29.228: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[40] 3GPP2 X.S0011: "cdma2000 Wireless IP Network Standard".

[41] 3GPP2 C.S0023: "Removable User Identity Module for Spread Spectrum Systems".

[42] Void.

[43] 3GPP2 S.S0055: "Enhanced Cryptographic Algorithms".

[44] 3GPP2 S.S0078: "Common Security Algorithms".

[45] 3GPP2 C.S0065: "cdma2000 Application on UICC for Spread Spectrum Systems".

[46] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification".

[47] Void.

[48] Void.

[49] Void.

[50] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2".

[51] 3GPP TS 31.103: "3rd Generation Partnership Project: Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[52] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[53] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[54] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[55] Void.

[56] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[57] ETSI TS 187 003 v3.4.1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[58] Void.

[59] Void.

[60] IETF RFC 6544: "TCP Candidates with Interactive Connectivity Establishment (ICE) ".

[61] Void.

[62] IETF RFC 6062: "Traversal Using Relays around NAT (TURN) Extensions for TCP Allocations".

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

[64] IETF RFC 6623: "Indication of Support for Keep-Alive".

[65] IETF RFC 4169: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2”.

[66] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[67] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[68] IETF RFC 7376: "Problems with Session Traversal Utilities for NAT (STUN) Long-Term Authentication for Traversal Using Relays around NAT (TURN)".

[69] Void.

[70] IETF RFC 7635: "Session Traversal Utilities for NAT (STUN) Extension for Third Party Authorization".

[71] Void

[72] IETF RFC 6749: "The OAuth 2.0 Authorization framework".

[73] IETF RFC 4106: "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)".

[74] IETF RFC 4543: "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH".

[75] IETF RFC 7800: "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)".

[Z1] IETF RFC 8489: "Session Traversal Utilities for NAT (STUN)".

[Z2] IETF RFC 8656: " Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[Z3] IETF RFC 8445: "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal".

[Z4] IETF RFC 8839: "Session Description Protocol (SDP) Offer/Answer Procedures for Interactive Connectivity Establishment (ICE)".

[Z5] IETF RFC 8981: "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6".

[Z6] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

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

### 6.1.1 Authentication of an IM-subscriber

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S‑CSCF, cf. figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.



Figure 4: The IMS Authentication and Key Agreement for an unregistered IM subscriber and successful mutual authentication with no synchronization error

The detailed requirements and complete registration flows are defined in TS 24.229 [8] and TS 24.228 [11].

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

|  |
| --- |
| SM1:REGISTER(IMPI, IMPU) |

In SM2 and SM3 the P‑CSCF and the I‑CSCF respectively forwards the SIP REGISTER towards the S‑CSCF.

After receiving SM3, if the IMPU is not currently registered at the S‑CSCF, the S‑CSCF needs to set the registration flag at the HSS to initial registration pending. This is done in order to handle UE terminated calls while the initial registration is in progress and not successfully completed. The registration flag is stored in the HSS together with the S‑CSCF name and user identity, and is used to indicate whether a particular IMPU of the user is unregistered or registered at a particular S‑CSCF or if the initial registration at a particular S‑CSCF is pending. The registration flag is set by the S‑CSCF sending a Cx-Put to the HSS. If the IMPU is currently registered, the S‑CSCF shall leave the registration flag set to *registered*. At this stage the HSS has performed a check that the IMPI and the IMPU belong to the same user.

Upon receiving the SIP REGISTER the S‑CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S‑CSCF has no valid AV then the S‑CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

|  |  |
| --- | --- |
| CM1:Cx-AV-Req(IMPI, m) |  |

Upon receipt of a request from the S‑CSCF, the HSS sends an ordered array of *n* authentication vectors to the S‑CSCF using CM2. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the S‑CSCF and the IMS user.

|  |  |
| --- | --- |
| CM2:Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn) |  |

When the S‑CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e. authentication vectors in a particular S‑CSCF are used on a first-in / first-out basis.

The S‑CSCF sends a SIP 4xx Auth\_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P‑CSCF. RFC 3310 [17] and RFC 4169 [65] specifies how to populate the parameters of an authentication challenge. The S‑CSCF shall offer both "AKAv2-SHA-256" [65] and "AKAv1-MD5" [17] starting with "AKAv2-SHA-256" as most preferred. The S‑CSCF also stores the RAND sent to the UE for use in case of a synchronization failure. To maintain backwards compatibility with pre Rel-17 releases, "AKAv1-MD5" is supported but not recommended to use.

The verification of the SQN by the USIM and ISIM will cause the UE to reject an attempt by the S‑CSCF to re-use a AV. Therefore no AV shall be sent more than once.

NOTE: This does not preclude the use of the normal SIP transaction layer re-transmission procedures.

|  |
| --- |
| SM4:4xx Auth\_Challenge(IMPI, RAND, AUTN, IK, CK) |

When the P‑CSCF receives SM5 it shall store the key(s) and remove that information and forward the rest of the message to the UE i.e.

|  |
| --- |
| SM6:4xx Auth\_Challenge(IMPI, RAND, AUTN) |

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in TS 33.102 [1]. If both these checks are successful the UE selects the first algorithm it supports and uses RES and some other parameters to calculate an authentication response. The UE must support "AKAv2-SHA-256". This response is put into the Authorization header and sent back to the registrar in SM7. RFC 4169 [65] and RFC 3310 [17] specify how to populate the parameters of the response for "AKAv2-SHA-256" and "AKAv1-MD5" respectively. It should be noted that the UE at this stage also computes the session keys CK and IK. To maintain backwards compatibility with pre Rel-17 releases, "AKAv1-MD5" is supported but not recommended to use.

|  |
| --- |
| SM7:REGISTER(IMPI, Authentication response) |

The P‑CSCF forwards the authentication response in SM8 to the I‑CSCF, which queries the HSS to find the address of the S‑CSCF. In SM9 the I‑CSCF forwards the authentication response to the S‑CSCF.

Upon receiving SM9 containing the response, the S‑CSCF retrieves the active XRES for that user and uses this to check the authentication response sent by the UE as described in RFC 3310 [17] and RFC 4169 [65]. If the check is successful then the user has been authenticated and the IMPU is registered in the S‑CSCF. If the IMPU was not currently registered, the S‑CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

It shall be possible to implicitly register IMPU(s). (see clause 4.3.3.4 in TS 23.228 [3]). All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S‑CSCF and subsequently to the P‑CSCF. The S‑CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

When an IMPU has been registered this registration will be valid for some period of time. Both the UE and the S‑CSCF will keep track on a timer for this purpose but the expiration time in the UE is smaller than the one in the S‑CSCF in order to make it possible for the UE to be registered and reachable without interruptions. A successful registration of a previously registered IMPU (including implicitly registered IMPUs) means the expiry time of the registration is refreshed.

If the user has been successfully authenticated, the S‑CSCF sends a SM10 SIP 2xx Auth\_OK message to the I-CSCF indicating that the registration was successful. In SM11 and SM12 the I‑CSCF and the P‑CSCF respectively forward the SIP 2xx Auth\_OK towards the UE.

It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with an incorrect authentication response in order to make the HN de-register the IMPU. For this reason a subscriber, when registered, shall not be de-registered if it fails an authentication.

The lengths of the IMS AKA parameters are specified in clause 6.3.7 of TS 33.102 [1].

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

## 7.5 Rules for security association handling when the UE changes IP address

When a UE changes its IP address, e.g. by using the method described in RFC 8981 [Z5], then the UE shall delete the existing SA's and initiate an unprotected registration procedure using the new IP address as the source IP address in the packets carrying the REGISTER messages.

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

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" / "aes-gmac" / "null" )

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

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

 encrypt-algorithm = "ealg" EQUAL ("aes-cbc" / "aes-gcm" / "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" and "null". Removal of "hmac-md5-96"

 "ealg" parameter: Addition of "aes-cbc" 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.

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

Annex I (normative):
Key expansion functions for IPsec ESP

**Integrity Keys:**

If the selected authentication algorithm is HMAC-SHA-1-96 then IKESP is obtained from IKIM by appending 32 zero bits to the end of IKIM to create a 160‑bit string.

If selected authentication algorithm is AES-GMAC as specified in RFC 4543 [74] with 128 bit key then IKESP = IKIM.

The salt value specified in Section 3.2 of RFC 4543 [74] shall be derived using the key derivation function KDF defined in Annex B of TS 33.220 [66]. The input Key to the KDF function shall be equal to the concatenation of CKIM and IKIM: CKIM || IKIM. The input S to the KDF function shall be formed from the following parameters:

- FC = 0x58.

- P0 = "AES\_GMAC\_SALT" .

- L0 = length of the string “AES\_GMAC\_SALT” (i.e. 0x00 0x0D).

The salt value shall consist of the 32 least significant bits of the 256 bits of the KDF output.

"Hmac-sha-1-96" is not recommended.

**Encryption Keys:**

If selected encryption algorithm is AES‑CBC as specified in RFC 3602 [22] with 128 bit key then CKESP = CKIM .

If selected encryption algorithm is AES‑GCM as specified in RFC 4106 [73] with 128 bit key then CKESP = CKIM. The salt value specified in Section 4 of RFC 4106 [73] shall be derived using the key derivation function KDF defined in Annex B of TS 33.220 [66]. The input Key to the KDF function shall be equal to the concatenation of CKIM and IKIM: CKIM || IKIM. The input S to the KDF function shall be formed from the following parameters:

- FC = 0x59

- P0 = “AES\_GCM\_SALT”

- L0 = length of the string “AES\_GCM\_SALT” (i.e. 0x00 0x0C)

The salt value shall consist of the 32 least significant bits of the 256 bits of the KDF output.

"aes-cbc" is not recommended.

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

## O.2.1 TLS Profile for TLS based access security

When the UE and the P-CSCF implement and use TLS as specified in the present Annex O, TLS shall be implemented and used according to the TLS profile specified in TS 33.310 [24], Annex E. For all TLS versions the provisions on ciphersuites given in TS 33.310 [24], Annex E, shall apply.

-

- Authentication of the P-CSCF

- The P-CSCF shall be authenticated by the UE by presenting a valid server certificate. The P-CSCF certificate profile shall be based on TLS certificates as presented in clause O.5.1.

- Authentication of the UE

- The P-CSCF shall not request a certificate in a Server Hello Message from the UE. The HN shall authenticate the UE as specified in Annex N of this specification.

- Verification of the TLS session endpoints

- In order for the UE to be able to trust the TLS session endpoint, the P-CSCF certificate shall be used during the authentication procedure.

- In order for the P-CSCF to be able to trust that the UE, which was authenticated according to Annex N, is the TLS session endpoint, the P-CSCF shall use the mechanism for associating the TLS Session ID with registration parameters IP address, port, IMPI, IMPU(s), specified in clause O.2.2, and shall have assurance that man-in-the-middle attacks can be mitigated, e.g. by following the rules in the NOTE in clause O.1.1.

- TLS session parameters

* The TLS Handshake Protocol negotiates a session, which is identified by a Session ID.

- The lifetime of a Session ID is subject to local policies of the UE and the P-CSCF. A recommended lifetime is one hour (or at least more than the re-REGISTRATION time out). The procedure for TLS session re-negotiation in IMS is specified in clauses O.4.1 and O.4.2.

- Ports

- The P-CSCF shall be prepared to accept TLS session requests on port 5061 or on a port published by the operator.

- Forwarding requests

- The procedures for forwarding requests by the edge proxy in RFC 5626 [32] shall apply to the P-CSCF when managing TLS connections.

NOTE 1: The use of RFC 5626 [32] in conjunction with TLS is needed so that terminating requests can re-use an existing TLS connection.

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

## S.5.3 Intra-domain Domain Security

The interface labeled 5 in Figure S.1 is between SIP-capable nodes in the same network security domain. The interface labeled 3 in Figure S.1 is between the I-CSCF/S-CSCF and the HSS. There may be other interfaces to nodes inside the Home Network, which are also intended to be covered by this clause. As these interfaces exist entirely within one network security domain, the administrative authority may choose any mechanism to secure this interface, including physical security where appropriate. Cryptographic methods of security, if applied, shall include both privacy and integrity protection, and be at least as strong as the IPsec (RFC 4301 [53], RFC 7296 [Z6]) profile defined in clause S.5.4.

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

#### S.5.4.2.1 General

For the interfaces security protection between IMS network elements, this clause specifies the protection using IPsec as specified in RFC 4301 [53]. The key management and distribution architecture is based on the IPsec IKE (RFC 4301 [53], RFC 7296 [Z6]) protocols. IKEv2 shall follow the 3GPP IKEv2 profile as defined in clause 5.4 of TS 33.210 [5] and clause 6.2.1b of TS 33.310 [24].

The security services provided by network domain security are:

- data integrity;

- data origin authentication;

- anti-replay protection;

- confidentiality (optional);

- limited protection against traffic flow analysis when confidentiality is applied.

The IPsec security protocol shall always be ESP. Integrity protection/message authentication together with anti-replay protection shall always be used. IPsec ESP should be used with both encryption and integrity protection for all SIP signaling traversing inter-security domain boundaries.

IPsec offers a set of security services, which is determined by the negotiated IPsec security associations. That is, the IPsec SA defines which security protocol to be used, the mode, and the endpoints of the SA.

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

#### S.5.4.2.2 Support of ESP authentication and encryption

For IMS signaling traffic, ESP shall always be used to provide data integrity, data origin authentication, and anti-replay protection services, thus the ESP\_NULL authentication algorithm shall not be allowed for use. ESP shall follow the 3GPP ESP profile as defined in clause 5.3 of TS 33.210 [5].

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

### W.3.1.2 Firewall traversal for IMS control plane using SIP over TLS/TCP

Firewall traversal for IMS control plane is accomplished by running SIP over TLS and using port 443 (HTTPS) instead of the standard port 5061 (SIPS). This makes the SIP signalling appear as HTTPS traffic to any firewall that is present along the signalling path.

In order to ensure that the firewall pinholes are maintained, the IMS client -shall apply the keep-alive mechanism specified in RFC 5626 [32]. The keep-alive mechanism is negotiated by the IMS client and the P-CSCF at IMS registration using the method described in RFC 6223 [64]. Note that RFC 5626 defines two keep-alive techniques: a technique based on STUN for connection-less transports and a technique based on SIP (called CRLF) for connection-oriented transports. Since TCP is used as transport between the IMS client and the P-CSCF, the CRLF keep-alive technique must be used.

In case the IMS client is configured to use an HTTP proxy, the IMS client uses the HTTP CONNECT method (see RFC 2817 [63]) to request the proxy to establish a TCP connection with the P-CSCF on its behalf. Once the client has received a positive reply from the proxy that the TCP connection has been established, the client initates the TLS handshake with the P-CSCF and establishes the TLS tunnel. Note that the use of the HTTP CONNECT method is completely transparent to P-CSCF.

Editor’s note: It needs to be verified that this does not interfere with the HTTP proxy settings on the UE.

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

### W.3.1.3 Firewall traversal for IMS media plane using ICE and TURN

Firewall traversal for IMS media plane is accomplished by using the ICE protocol together with an enhanced version of TURN. ICE is defined in RFC 8445 [Z3] and RFC 8839 [Z4] and is a protocol for performing NAT traversal of UDP based media streams. ICE in turn makes use of TURN, defined in RFC 5766 [60], which is a protocol for relaying media through a relay server. An IMS client that supports ICE will allocate relayed candidates at the TURN server and include the candidate information in the SDP offer/answer sent to the peer. The relayed candidates will be used as a last resort when the client and peer fail to establish a direct communication path. The communication between the client and the TURN server (this includes both the relayed media and the control information needed to setup the relayed candidates) can occur over UDP, TCP or TCP/TLS. By using TCP/TLS on port 443 (HTTPS) or TCP on port 80 (HTTP) the communication will appear as HTTP(S) to firewalls and will (typically) be allowed through. Using TCP instead of TLS/TCP reduces the overhead but will fail when the firewall performs DPI or if an HTTP proxy is present. An IMS client may be configured to use both TURN over TCP/80 and TURN over TLS/443, in such case, the client should prefer to use TURN over TCP/80 to avoid TLS overhead.

ICE and TURN have later on been extended to also support TCP based media. ICE TCP is defined in RFC 8445 [Z3] and RFC 8839 [Z4] and TURN TCP is defined in RFC 8656 [Z2]. One of the changes introduced in TURN TCP is that the multiple TCP connections are established between the client and TURN server: one for exchange of control information and one for each relayed TCP based media stream. All UDP based media streams are relayed over the same TCP connection that is used for the control information, just as in the original TURN protocol. The TURN server will use TCP/TLS on port 443 (HTTPS) or TCP over port 80 (HTTP) for all the connections. In order to reduce the TLS setup time when several TCP connections are established, the IMS client and TURN server may use the TLS session resumption feature.

An IMS client that is configured to use an HTTP proxy uses the HTTP CONNECT method (see RFC 2817 [63]) to request the proxy to establish a TCP connection with the TURN server. Once the client has received a positive reply from the proxy that the TCP connection has been established, the client initates the TLS handshake with the TURN server and establishes the TLS tunnel. This procedure is repeated once for every TCP connection the client establishes with the TURN server. Note that the use of the HTTP CONNECT method is completely transparent to TURN server.

Using ICE for firewall traversal is particularly suitable for IMS clients that already implement ICE for NAT traversal, since in this case only minimal changes are required to the client. Usage of ICE for IMS clients is specified in TS 23.228 [3] and TS 24.229 [8].

Note that there is no need to specify any keep-alive mechanism since this functionality is already included in ICE. The IMS client will send regular STUN keep-alives which ensures that the firewall pinholes are maintained.

Editor's note: ICE TCP is required for TCP based media (e.g. MSRP) but is not yet supported in TS 23.228 [3] and TS 24.229 [8]. These specifications need to be updated.

Editor's note: How the client is authenticated and authorized by the TURN server is ffs. One possibility is to use the SIP Digest credentials and the normal TURN authentication procedure. However, this would require an additional interface between the TURN server and the HSS. Another possibility is to use GBA but this would perhaps be unnecessarily complex considering that the only attack we need to protect against is DoS.

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

## W.3.3 Required functions of the UE

For firewall traversal of IMS control plane, the IMS client shall implement the following functionality:

- support SIP over TLS/TCP on the non-standard port 443 (HTTPS);

- support the SIP Digest authentication method according to Annex N;

- support the CRLF keep-alive technique defined in RFC 5626 [32] together with the negotiation mechanism defined in RFC 6223 [64];

- support the HTTP CONNECT method in RFC 2817 [63] for establishing the TLS tunnel with the P-CSCF when the IMS client is configured with an HTTP proxy.

For firewall traversal of IMS media plane, the IMS client shall implement the following functionality:

- support ICE for UDP and TCP based media streams according to Annex G of TS 23.228 [3];

- support TLS/TCP on non-standard port 443 and TCP on non-standard port 80 for communication with TURN server;

- support the HTTP CONNECT method in RFC 2817 [63] for establishing TLS tunnels with the TURN server when the IMS client is configured with an HTTP proxy.

Note that the HTTP CONNECT method is only used when the IMS client is configured with an HTTP proxy for outgoing HTTP(S) requests. The way in which the IMS client obtains the proxy address and port is out of scope.

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

### X.2.2.3 Procedures

Figure X.2.3-1 shows the registration flow. In this figure SIP over secure WebSocket is used between the WIC and the eP-CSCF. Other protocols (e.g. HTTP RESTful or JSON over WebSocket) can also be used as long as it is able to relay the digest challenge, challenge-response, and auth-info values.

 Solution 1.1 requires that the IMPU and SIP Digest password are made available to the JavaScript in the WIC. The IMPI can be omitted from the initial SIP Register request, and if that is the case the S-CSCF will try to determine its value from the registering IMPU. This requires that IMPUs are not shared between IMS users (see Annex N).

NOTE 1: It is assumed that the credentials are entered by the user via the web GUI or retrieved from the WWSF over HTTPS. Note that the latter option requires that WWSF has authenticated the user previously.

NOTE 2: Unless the SIP Digest password or the intermediate hash value H(A1) (see RFC 7235 [Z7] and RFC 7616 [Z9]) is stored in the WIC, the password needs to be re-obtained each time a re-registration is performed. If the password is entered manually and if re-registrations occur often, this will result in a negative user experience. This can be avoided by storing the SIP Digest password or H(A1) in the WIC after the initial registration procedure. Ensuring the confidentiality of the SIP Digest password or H(A1) during storage is at the discretion of the implementation and is outside the scope of 3GPP. The use of MD5 in HTTP Digest is not recommended and only supported for interop with Rel-16 and older releases.

NOTE 3: It is recommended that the user does not enter his SIP Digest credentials into the WIC, except possibly once before the initial registration.



Figure X.2.2.3-1: WebRTC IMS Client authentication using SIP Digest

The details of the signalling flows are as follows:

1) **Web page download from WWSF**

From within a WebRTC-enabled browser, the user accesses a URI to the WWSF to initiate an HTTPS connection to the WWSF. The TLS connection provides one-way authentication of the server based on the server certificate. The browser downloads and initializes the WIC from the WWSF.

**2) Establishment of secure Web socket connection between WIC and eP-CSCF**

The WIC opens a WSS (secure Web Socket) connection to the eP-CSCF. The TLS connection provides one-way authentication of the server based on the server certificate. The eP-CSCF verifies in this step that the WIC establishing the signalling connection comes from a trusted domain.

NOTE 3: The protection mechanism works under the assumption that the browser is not under the attacker's control.

**3-10) SIP Digest message flow**

The SIP Digest messages exchanged between the WIC and eP-CSCF and between the eP-CSCF and the I/S-CSCF are as defined in Annex N of this document.

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

## X.5.1 Introduction

TURN RFC 8656 [Z2] specifies that TURN servers and clients MUST implement "Long-Term Credential Mechanism" as specified in clause 10.2 of RFC 8489 [Z1]. In this mechanism, the client and server share a pre-provisioned username and password that remains in the system till the user is using the system.The TURN server uses these credentials to authenticate the client by performing digest challenge/response.

In IMS\_WebRTC, the browser plays the role of a TURN client. The WIC (i.e. the Javascript code) controls the execution of the browser via the W3C defined RTCPeerConnection API. Through this API, the WIC provides TURN credentials to the browser. These credentials should therefore be made available to the WIC.

There are two known gaps that need to be addressed before TURN can be used in IMS\_WebRTC:

1) At present, the provisioning of TURN long-term credentials in the WIC is un-defined.

2) Moreover, as indicated in RFC 7376 [68], ensuring secrecy of these credentials in a web-based application such as the WIC is difficult. Once these credentials are exposed to a Javascript script, it could lead to various security issues such as leak of the credentials, privacy leakage etc.

A solution is needed to dynamically configure the TURN credentials in the WIC while ensuring that security gaps identified by RFC 7376 [68] are addressed.

Two solutions are presented in this annex for TURN credential provisioning and authentication:a) eP-CSCF based dynamic provisioning of credentials in the WIC and TURN server

b) TURN client authentication based OAuth 2.0 access tokens.

Both solutions are optional for implementation.

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

## X.5.2 Solution 1: TURN credential provisioning and authentication using eP-CSCF

### X.5.2.1 Overview

This solution reuses the TURN long-term credential method defined in RFC 8656 [Z2] , but the credential is dynamically provisioned by eP-CSCF via the signalling channel. When WIC registers to IMS, WIC requests the IMS networks to provision a credential for TURN authentication using a 3GPP extension header. If the request is authenticated and authorized, eP-CSCF generates a TURN credential, including user id, password, expiration, etc, and sends the credential to WIC in the response message. Since the signaling messages between WIC and eP-CSCF are protected by the secure protocols, e.g. secure Websocket, the TURN credential is securely transferred to WIC. The WIC retrieves the credential and uses it in subsequent TURN allocation requests. The WIC may request TURN credential for every registration, or use the credential until it expires. WIC can also use other signaling messages such as OPTION to request a new credential at anytime before re-registration.

This method requires some enhancement of WIC and eP-CSCF. WIC needs to be enhanced to use the 3GPP extension header to request TURN credential from eP-CSCF via signaling messages. The eP-CSCF needs to be enhanced to process TURN credential request and generate TURN user name and password using a preshared key with the TURN server. The TURN server also needs to be enhanced to re-generate TURN password from username in TURN request and the preshared key with P-CSCF.

This solution provides a way to provision TURN credential in large scale with minor change to existing functions. It addresses the security issues in 8489 [Z1] by dynamically generating TURN user name and password. This solution is optional to support. When to use this solution depends on WebRTC deployment scenario and operator’s policy. For example, if a deployment does not have WAF, or if the WAF or TURN server does not support TURN access token, the eP-CSCF based approach may be used for TURN credential provision and authentication since the alternative solution requires the use of WAF and support of TURN access token by TURN server, WAF.

### X.5.2.2 Procedures

The procedure of TURN credential provision via eP-CSCF is shown in figure X.5.2.2.1. To use this solution, a shared secret key *Km* should be configured between eP-CSCF and TURN server using out of band method not defined in this solution.

1) WIC establishes secure websocket with eP-CSCF

2) WIC sends REGISTER request to eP-CSCF with 3GPP extended header (3gpp-ext-turn-cred) for TURN credential request.

3) eP-CSCF authenticate and authorized the request then

1) Generate a random user ID *Tid* and credential expiration time *Texp* based on its policy, *Tid* and *Texp should be encoded as string type.*

2) Generate TURN password using *Km*, *Tpwd* = HASH (*Km* , *Tid : Texp* )

4) eP-CSCF sends REGISTER response with generated TURN credential using the 3gpp extended header. The valud of the header = (*Tid : Texp : Tpwd),*  which is the concatenation of *Tid, Texp, Tpwd* separated by semi-colon sign.

5) IC extracts the TURN credential from the TURN credential header. The WIC uses (*Tid : Texp)* as TURN USERNAME and uses *Kpwd* to compute the MESSAGE-INTEGRITY value of TURN Allocate request as defined in IETF RFC 8656 [Z2].

6) TURN server re-generates TURN password using the USERNAME attribute in request and the preshared key with eP-CSCF

7) TURN server validates that the credential has not expired and verifies the integrity of the TURN request using the password generated in step 6.

8) TURN server sends Allocate response with allocated relay address to WIC

The procedure above uses REGISTER as example to explain how to request TURN credential from eP-CSCF by signaling messages. WIC may use other signaling messages, such as OPTIONAL, to request TURN credential.



 Figure X.5.2.2-1: TURN Credential provisioned by eP-CSCF

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