**3GPP TSG-SA3 Meeting #101-e *S3-203315-r2***

**e-meeting, 9th - 20th November 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **1017** | **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 |  | Radio Access Network | **X** | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Correcting use of (D)TLS in 33.501 |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI16 |  | ***Date:*** | 2020-10-30 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***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:*** | - None of the uses of (D)TLS have a certificate profile. Some of the interfaces are missing text on certificates while other refer to the TLS profile in TS 33.210 which does not contain any certificate profile.- The TLS profile has been moved to TS 33.210.- The authentication method in RFC 4279 is forbidden to support.- The SBA profile does not actually specifies that it used HTTPS. HTTP over TLS is not HTTPS unless it follow RFC 2818. All CT1 SBA examples use the https:// uri.- TLS protection of DNS is not refering to the 3GPP TLS profile.- The Diameter RFC 6733 has a horrible TLS profile mandating TLS\_RSA\_WITH\_RC4\_128\_MD5 and allowing SSL 3.0.- NDS/IP and the IPsec RFC has a lot of requirements and considerations on mutual authentication using identities in the certificates, and how identies are used for authorization and security policies. The 3GPP TLS profile and the TLS RFCs completely lack any requirement on authentication due to the fact the TLS is used in variety of use cases, some using oportunistic encryption. This seems to have been overlooked when (D)TLS was introduces as an alternative to NDS/IP. |
|  |  |
| ***Summary of change:*** | - Specified that the certificate profile given in clause 6.1.3a of TS 33.310 shall be used for all interfaces using (D)TLS.- Replaced RFC 4279 with RFC 5489- Updated reference to TLS profile in TS 33.210- Specified that SBA use HTTPS and refer to RFC 2818.- Added TLS and certificate profile for DNS and Diameter- Added explicit text on mutual authentication and policy checks for all interfaces using the identities in the end entity certificates. |
|  |  |
| ***Consequences if not approved:*** | - Risk for incompatable implementations as none of the (D)TLS uses have a certificate profile. - Risk that 5G critical infrastucture with very low security due to weak algorithms in the X.509 certificate, weak protocol versions like SSL 3.0, or weak cipher suites like the profile in RFC 6733, or no mutual authentication. |
|  |  |
| ***Clauses affected:*** | 2, 9.2, 9.4, 9.5, 9.8.2, 9.8.3, 12.2, 13.1.0, 13.1.2, 15.2, 15.3, Annex B.2.1.1,  |
|  |  |
|  | **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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

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

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

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

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[12] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

Editor’s note: This reference will be removed and references to it updated when the IETF updates the RFC and publishes a new RFC that supercedes this RFC.

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

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

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

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

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void.

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] Internet draft draft-ietf-emu-rfc5448bis: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.500: "Technical Realization of Service Based Architecture".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

[77] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

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

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

## 9.2 Security mechanisms for the N2 interface

N2 is the reference point between the AMF and the 5G-AN. It is used, among other things, to carry NAS signalling traffic between the UE and the AMF over 3GPP and non-3GPP accesses.

The transport of control plane data over N2 shall be integrity, confidentiality and replay-protected.

In order to protect the N2 reference point, it is required to implement IPsec ESP and IKEv2 certificates-based authentication as specified in sub-clause 9.1.2 of the present document. IPsec is mandatory to implement on the gNB and the ng-eNB. On the core network side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect N2 is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

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

## 9.4 Security mechanisms for the Xn interface

Xn is the interface connecting NG-RAN nodes. It consists of Xn-C and Xn-U. Xn-C is used to carry signalling and Xn-U user plane data.

The transport of control plane data and user data over Xn shall be integrity, confidentiality and replay-protected.

In order to protect the traffic on the Xn reference point, it is required to implement IPsec ESP and IKEv2 certificate- based authentication as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection. IPsec shall be supported on the gNB and ng-eNB.

In addition to IPsec, for the Xn-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding..

NOTE 2: The use of cryptographic solutions to protect Xn is an operator's decision. In case the NG-RAN node (gNB or ng-eNB) has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the NG-RAN node.

QoS related aspects are further described in sub-clause 9.1.3 of the present document.

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

## 9.5 Interfaces based on DIAMETER or GTP

This clause applies to all DIAMETER or GTP-based interfaces between the 5G Core and other network entities that are not part of the 5G System. These includes the Rx interface between the PCF and the IMS System and the N26 interface between the AMF and the MME.

The protection of these interfaces shall be supported according to NDS/IP as specified in TS 33.210 [3], unless security is provided by other means, e.g. physical security. If (D)TLS is used, implementation and usage shall follow the profile given in clause 6.2 of TS 33.210 [3] and clause 6.1.3a of TS 33.310 [5]. The cipher suites in RFC 6733 shall not be supported. A SEG may be used to terminate the NDS/IP IPsec tunnels.

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

### 9.8.2 Security mechanisms for the F1 interface

The F1 interface connects the gNB-CU to the gNB-DU. It consists of the F1-C for control plane and the F1-U for the user plane. The security mechanisms for the F1 interface connecting the IAB-node to the IAB-donor-CU are detailed in clause M.3.3 of this document.

In order to protect the traffic on the F1-U interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In order to protect the traffic on the F1-C interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

IPsec is mandatory to implement on the gNB-DU and on the gNB-CU. On the gNB-CU side, a SEG may be used to terminate the IPsec tunnel.

In addition to IPsec, for the F1-C interface, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect F1 is an operator's decision. In case the gNB or the IAB-node has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB or the IAB-node.

NOTE 3: The security considerations for DTLS over SCTP are documented in RFC 6083 [58].

NOTE 4: The support of DTLS for F1-C, between the IAB-node (gNB-DU) and the IAB-donor-CU, is optional for the IAB-node and the IAB-donor-CU.

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

### 9.8.3 Security mechanisms for the E1 interface

The E1 interface connects the gNB-CU-CP to the gNB-CU-UP. It is only used for the transport of signalling data.

In order to protect the traffic on the E1 interface, IPsec ESP and IKEv2 certificates-based authentication shall be supported as specified in sub-clause 9.1.2 of the present document with confidentiality, integrity and replay protection.

In addition to IPsec, DTLS shall be supported as specified in RFC 6083 [58] to provide mutual authentication, integrity protection, replay protection and confidentiality protection. Security profiles for DTLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

IPsec is mandatory to support on the gNB-CU-UP and the gNB-CU-CP. Observe that on both the gNB-CU-CP and the gNB-CU-UP sides, a SEG may be used to terminate the IPsec tunnel.

NOTE 1: The use of transport layer security, via DTLS, does not rule out the use of network layer protection according to NDS/IP as specified in TS 33.210 [3]. In fact, IPsec has the advantage of providing topology hiding.

NOTE 2: The use of cryptographic solutions to protect E1 is an operator's decision. In case the gNB has been placed in a physically secured environment then the 'secure environment' includes other nodes and links beside the gNB.

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

## 12.2 Mutual authentication

For authentication between NEF and an Application Function that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates shall be performed between the NEF and AF using TLS.

Certificate based authentication shall follow the profiles given in 3GPP TS 33.310 [5], clause 6.1.3a. The identities in the end entity certificates shall be used for authentication and policy checks. The structure of the PKI used for the certificate is out of scope of the present document.

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

### 13.1.0 General

All network functions shall support mutually authenticated TLS and HTTPS as specified in RFC 7540 [47] and RFC 2818 [XX]. The identities in the end entity certificates shall be used for authentication and policy checks. Network functions shall support both server-side and client-side certificates. TLS client and server certificates shall be compliant with the SBA certificate profile specified in clause 6.1.3c of TS 33.310 [5].

The TLS profile shall follow the profile given in clause 6.2 of TS 33.210 [3] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

TLS shall be used for transport protection within a PLMN unless network security is provided by other means.

NOTE 1: Regardless of whether TLS is used or not, NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5] can be used for network layer protection.

NOTE 2: If interfaces are trusted (e.g. physically protected), it is for the PLMN-operator to decide whether to use cryptographic protection.

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

### 13.1.2 Protection between SEPPs

If there are no IPX entities between the SEPPs, TLS shall be used between the SEPPs. If there are IPX entities between SEPPs, PRINS (application layer security on the N32-f interface) shall be used for protection between the SEPPs. PRINS is specified in clause 5.9.3 (requirements) and clause 13.2 (procedures).

NOTE 1a: The procedure specified in clause 13.5 for security mechanism selection between SEPPs provides robustness and future-proofness, e.g. in case new algorithms are introduced in the future.

If PRINS is used on the N32-f interface, one of the following additional transport protection methods should be applied between SEPP and IPX provider for confidentiality and integrity protection:

- NDS/IP as specified in TS 33.210 [3] and TS 33.310 [5], or

- TLS VPN with mutual authention following the profile given in clause 6.2 of TS 33.210 [3] and clause clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks, with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [47].

NOTE 1: Void

NOTE 2: Void.

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

## 15.2 Mutual authentication

If a management service consumer resides outside the 3GPP operator’s trust domain, mutual authentication shall be performed between the management service consumer and the management service producer using TLS. TLS shall follow the profile given in 3GPP TS 33.210 [3], clause 6.2 and either 1) the client and server certificates with the profiles given in 3GPP TS 33.310 [5], clause 6.1.3a or 2) pre-shared keys following RFC 5489for TLS 1.2 and RFC 8446 [60] for TLS 1.3. The structure of the PKI used for the certificates is out of scope of the present document. The identities in the end entity certificates shall be used for authentication and policy checks. The key distribution of pre-shared keys for TLS is up to the operator’s security policy and out of scope of the present document.

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

## 15.3 Protection of management interactions between the management service consumer and the management service producer

TLS shall be used to provide mutual authentication, integrity protection, replay protection and confidentiality protection for the interface between the management service producer and the management service consumer residing outside the 3GPP operator’s trust domain. Security profiles for TLS implementation and usage shall follow the TLS profile given in clause 6.2 of TS 33.210 [3] and the certificate profile given in clause 6.1.3a of TS 33.310 [5]. The identities in the end entity certificates shall be used for authentication and policy checks.

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

### B.2.1.1 Security procedures

EAP-TLS is a mutual authentication EAP method that can be used by the EAP peer and the EAP server to authenticate each other. It is specified in RFC 5216 [38] and draft-ietf-emu-eap-tls13 [76]. The 3GPP TLS protocol profile related to supported TLS versions and supported TLS cipher suites in 3GPP networks is specified in clause 6.2 of TS 33.210 [3]. The 3GPP profile of TLS certificates is specified in clause 6.1.3a of TS 33.310 [5].

EAP-TLS supports several TLS versions, and the negotiation of the TLS version is part of EAP-TLS. The main principle of negotiation goes as follows. The EAP server indicates the support for EAP-TLS in the EAP-Request. If the peer chooses EAP-TLS, it responds with an EAP-Response indicating in the ClientHello message which TLS versions the peer supports. The EAP server chooses the TLS version, and indicates the chosen version in the ServerHello message.

The TLS procedure described in the RFC 5216 [38] is applicable to TLS 1.2 defined in RFC 5246 [40]. The TLS procedure described in the draft-ietf-emu-eap-tls13 [76] is applicable to TLS 1.3 defined in RFC 8446 [77].

The procedure below is based on the unified authentication framework from the present document, procedures from TS 23.502 [8] and RFC 5216 [38]. The procedure for EAP-TLS with TLS 1.2 is presented here as an example, and other potential procedures are possible, e.g. if TLS resumption is used.



Figure B.2.1.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial authentication

1. The UE sends the Registration Request message to the SEAF, containing SUCI. If the SUPI is in NAI format, only the username part of the NAI is encrypted using the selected protection scheme and included in the SUCI, together with the realm part in the NAI needed for UDM routing.

Privacy considerations are described in Clause B.2.2.

2. The SEAF sends Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. The SUCI and the serving network name (as described in clause 6.1.1.4) are included in the message.

3. AUSF sends the the Nudm\_UEAuthentication\_Get Request, containing SUCI and the serving network name, to UDM. The general rules for UDM selection apply.

4. The SIDF located within the UDM de-conceals the SUCI to SUPI if SUCI is received in the message. The UDM then selects the primary authentication method.

5. If the UDM chooses to use EAP-TLS, it sends the SUPI and an indicator to choose EAP-TLS to AUSF in the Nudm\_UEAuthentication\_Get Response.

6. With the received SUPI and the indicator, the AUSF chooses EAP-TLS as the authentication method. The AUSF sends thea Nausf\_UEAuthentication\_Authenticate Response message containing EAP-Request/EAP-TLS [TLS start] message to the SEAF.

7. The SEAF forwards the EAP-Request/EAP-TLS [TLS start] in the Authentication Request message to the UE. This message also includes the ngKSI and the ABBA parameter. In fact, the SEAF shall always include the ngKSI and ABBA parameter in all EAP-Authentication request message. ngKSI will be used by the UE and AMF to identify the partial native security context that is created if the authentication is successful. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. During an EAP authentication, the value of the ngKSI and the ABBA parameter sent by the SEAF to the UE shall not be changed.

8. After receiving the EAP-TLS [TLS-start] message from SEAF, the UE replies with an EAP-Response/EAP-TLS [client\_hello] to the SEAF in the Authentication Response message. The contents of TLS client\_hello are defined in the TLS specification of the TLS version in use.

NOTE1: The EAP framework supports negotiation of EAP methods. If the UE does not support EAP-TLS, it should follow the rule described in RFC 3748 [27] to negotiate another EAP method. In 5G system, UDM typically knows which EAP method and credentials are supported by the subscriber, and consequently EAP based negotiation may never be used.

9. The SEAF forwards the EAP-Response/EAP-TLS [client hello] message to AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

10. The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf\_UEAuthentication\_Authenticate Response, which further includes information elements such as server\_hello, server\_certificate, server\_key\_exchange, certificate\_request, server\_hello\_done. These information elements are defined in the RFCs for the corresponding TLS version in use.

11. The SEAF forwards the EAP-Request/EAP-TLS message with server\_hello and other information elements to the UE through Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

12. The UE authenticates the server with the received message from step 11.

NOTE 2: The UE is required to be pre-configured with a UE certificate and also certificates that can be used to verify server certificates.

13. If the TLS server authentication is successful, then the UE replies with EAP-Response/EAP-TLS in Authentication Response message, which further contains information element such as client\_certificate, client\_key\_exchange, client\_certificate\_verify, change\_cipher\_spec, client\_finished etc. Privacy considerations are described in Clause B.2.1.2.

14. The SEAF forwards the message with EAP-Response/EAP-TLS message with client\_certificate and other information elements to the AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

15. The AUSF authenticates the UE based on the message received. The AUSF verifies that the client certificate provided by the UE belongs to the subscriber identified by the SUPI. If there is a miss-match in the subscriber identifiers in the SUPI, the AUSF does not accept the client certificate. If the AUSF has successfully verified this message, the AUSF continues to step 16, otherwise it returns an EAP-failure.

NOTE 2: The AUSF is required to be pre-configured with the root or any intermediary CA certificates that can be used to verify UE certificates. Deployment of certificate revocation lists (CRLs) and online certificate status protocol (OCSP) are described in clause B.2.2.

16. The AUSF sends EAP-Request/EAP-TLS message with change\_cipher\_spec and server\_finished to the SEAF in the Nausf\_UEAuthentication\_Authenticate Response.

17. The SEAF forwards EAP-Request/EAP-TLS message from step 16 to the UE with Authentication Request message. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1.

18. The UE sends an empty EAP-TLS message to the SEAF in Authentication Response message.

19. The SEAF further forwards the EAP-Response/EAP-TLS message to the AUSF in the Nausf\_UEAuthentication\_Authenticate Request.

20. The AUSF uses the most significant 256 bits of EMSK as the KAUSF and then calculates KSEAF from KAUSF as described in Annex A.6. The AUSF sends an EAP-Success message to the SEAF together with the SUPI and the derived anchor key in the Nausf\_UEAuthentication\_Authenticate Response.

21. The SEAF forwards the EAP-Success message to the UE and the authentication procedure is finished. This message also includes the ngKSI and the ABBA parameter. The SEAF shall set the ABBA parameter as defined in Annex A.7.1. Then the SEAF derives the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7, and provides the ngKSI and the KAMF to the AMF.

On receiving the EAP-Success message, the UE derives EMSK and uses the most significant 256 bits of the EMSK as the KAUSF and then calculates KSEAF in the same way as the AUSF. The UE derives the KAMF from the KSEAF, the ABBA parameter and the SUPI according to Annex A.7.

NOTE 3: Step 21 could be NAS Security Mode Command or Authentication Result.

NOTE 4: The ABBA parameter is included to enable the bidding down protection of security features that may be introduced later.

NOTE 5: As an implementation option, the UE creates the temporary security context as described in step 21 after receiving the EAP message that allows EMSK to be calculated. The UE turns this temporary security context into a partial security context when it receives the EAP Success. The UE removes the temporary security context if the EAP authentication fails.

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