Extended Subscriber Authentication Technical Specifications

CBRSA-TS-1003

V2.0.0

11 Jan 2019

LEGAL DISCLAIMERS AND NOTICES

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

Table of Contents

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

List of Figures

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

List of Tables

CBRS Alliance
3855 SW 153rd Drive
Beaverton, OR 97003
www.cbrsalliance.org
info@cbrsalliance.org

1 Introduction and Scope

This document defines UE and service provider procedures for extended subscriber authentication methods: Certificate Based Subscriber authentication (CBSA) and non-Certificate Based Subscriber Authentication. These extended authentication mechanisms are defined for both the NHN and the 3GPP-based Access Mode (non-EPS-AKA). The Stage 2 and 3 aspects are described in CBRSA-TS-1002 [3].

1.1 Key Words

The key words "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC-2119 [7]. In addition, the key word “conditional” shall be interpreted to mean that the definition is an absolute requirement of this specification only if the stated condition is met.

2 References

[1] CBRSA-TR-1001, “CBRS Network Services Technical Report”, v1.0.0. (Deprecated)

[2] CBRSA-TS-1001, “CBRS Network Services Requirements Technical Specification”, v 2.0.0 (Release 2), December 2018.

[3] CBRSA-TS-1002, “CBRS Network Services Technical Specification Stage 2 and 3”, v 2.0.0 (Release 2) <publication date TBD>

[4] IETF RFC 5448, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA’) ”, May 2009. https://tools.ietf.org/html/rfc5448.

[5] IETF RFC 5216, “The EAP-TLS Authentication Protocol”, March 2008. https://tools.ietf.org/html/rfc5216.

[6] MFA TS MF.202, MulteFire Alliance (MFA), “Architecture for Neutral Host Network Access Mode Stage 2 (Release 1)”, V1.0.3, June 2017.

[7] IETF RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, March 1997. https://tools.ietf.org/html/rfc2119.

[8] IETF RFC 5281, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)”, August 2008. https://tools.ietf.org/html/rfc5281.

[9] IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008. https://tools.ietf.org/html/rfc5280. (Deprecated)

[10] IETF RFC 2759, "Microsoft PPP CHAP Extensions", Version 2, January 2000. https://tools.ietf.org/html/rfc2759.

[11] IETF RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 1999. https://tools.ietf.org/html/rfc2560. (Deprecated)

[12] IETF RFC 5019, "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments", September 2007. https://tools.ietf.org/html/rfc5019. (Deprecated)

[13] IETF RFC 6960, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 2013. https://tools.ietf.org/html/rfc6960. (Deprecated)

[14] IETF RFC 6961, "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension", June 2013. https://tools.ietf.org/html/rfc6961. (Deprecated)

[15] IETF RFC 5247, "Extensible Authentication Protocol (EAP) Key Management Framework", August 2008. https://tools.ietf.org/html/rfc5247.

[16] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", v14.3.0, March 2017.

[17] 3GPP TS 33.401 "3GPP System Architecture Evolution: Security Architecture". v14.3.0, June 2017.

[18] 3GPP TS 23.122, "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode", v14.3.0, June 2017. (Deprecated)

[19] 3GPP TS 36.304, "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode", v14.3.0, June 2017. (Deprecated)

[20] 3GPP TS 36.331, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification", v14.3.0, July 2017. (Deprecated)

[21] 3GPP TS 33.402, "3GPP System Architecture Evolution (SAE): Security aspects of non-3GPP accesses", v14.3.0, September 2017. (Deprecated)

[22] 3GPP TS 29.273, "Evolved Packet System (EPS): 3GPP EPS AAA Interfaces", v14.3.0, June 2017.

[23] 3GPP TS 23.402, "Architecture enhancements for non-3GPP accesses", v14.3.0, March 2017. (Deprecated)

[24] 3GPP TS 24.301, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)", v14.3.0, March 2017. (Deprecated)

[25] National Security Agency (NSA). Commercial National Security Algorithm Suite (CNSA), available at https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm (Deprecated)

[26] IETF RFC 3748, "Extensible Authentication Protocol (EAP)", June 2004. https://tools.ietf.org/html/rfc3748.

[27] IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008. https://tools.ietf.org/html/rfc5246.

[28] IETF RFC 7170, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", May 2014. https://tools.ietf.org/html/rfc7170. (Deprecated)

[29] IETF RFC 7170, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)", May 2007. https://tools.ietf.org/html/rfc7170. (Deprecated)

[30] Microsoft Corporation, "[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)", February 2014. (Deprecated)

[31] IETF RFC 6678, "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method", July 2012. https://tools.ietf.org/html/rfc6678. (Deprecated)

[32] MFA TS 24.301, MulteFire Alliance (MFA), "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) Stage 3 (Release 1)", V1.0.2, February 2017.

[33] IETF RFC 3579, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", September 2003. https://tools.ietf.org/html/rfc3579.

[34] IETF RFC 6733, "Diameter Base Protocol", October 2012. https://tools.ietf.org/html/rfc6733.

[35] IETF RFC 7075, "Realm-Based Redirection In Diameter", November 2013. https://tools.ietf.org/html/rfc7075.

[36] IETF RFC 7542, "The Network Access Identifier", May 2015. https://tools.ietf.org/html/rfc7542.

[37] IETF RFC 4346, "The Transport Layer Security (TLS) Protocol Version 1.1", April 2006. https://tools.ietf.org/html/rfc4346. (Deprecated)

[38] IETF RFC 2246, "The TLS Protocol Version 1.0", January 1999. https://tools.ietf.org/html/rfc2246. (Deprecated)

[39] 3GPP TS 23.003, Third Generation Partnership Project (3GPP). "*Numbering, addressing and identification",* v14.3.0, March 2017. (Deprecated)

[40] IETF RFC 2548, "The Internet Engineering Task Force (IETF)". Microsoft Vendor-specific RADIUS Attributes, March 1999. https://tools.ietf.org/html/rfc2548.

[41] IETF RFC 6929, "Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions", April 2013. https://tools.ietf.org/html/rfc6929.

3 Definitions and Abbreviations

3.1 Abbreviation

AAA	Authentication, authorization and accounting
AKA	Authentication and Key Agreement
CBRS	Citizens Broadband Radio Service
CBSA	Certificate Based Subscribers Authentication
CA	Certification Authority
CRL	Certificate Revocation List
CSG	Closed Subscriber Group
EAP	Extensible Authentication Protocol
EE	End Entity
EMSK	Extended MSK
EPS	Evolved Packet System
IMSI	International Mobile Subscriber Identity
MME	Mobility Management Entity
MNO	Mobile Network Operator
MSB	Most Significant Bit
MSK	Master Session Key
NAI	Network Access Identifier
NAS	Non-Access Stratum
NH	Neutral Host
NHN	Neutral Host Network

NW	Network
OCSP	Online Certificate Status Protocol
OSU	Online Sign Up
PKI	Public Key Infrastructure
PSP	Participating Service Provider
PLMN	Public Land Mobile Network
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
SDP	Service Discovery Protocol
SMC	Security Mode Command
SIM	Subscriber Identity Module
SP	Service Provider
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UE	User Equipment
USIM	Universal Subscriber Identity Module

3.2 Definitions

Definitions are provided in [2].

4 Extended Subscriber Authentication

4.1 General

This document specifies extended subscriber authentication mechanisms, which are done using EAP from UE to MME (EAP over NAS) and from the MME to the AAA (EAP over Diameter/RADIUS), for both NHN Access Mode [2] and 3GPP-based Access Mode (non-EPS-AKA) [2]. In both cases, the call flow for EAP is depicted in Figure 1:

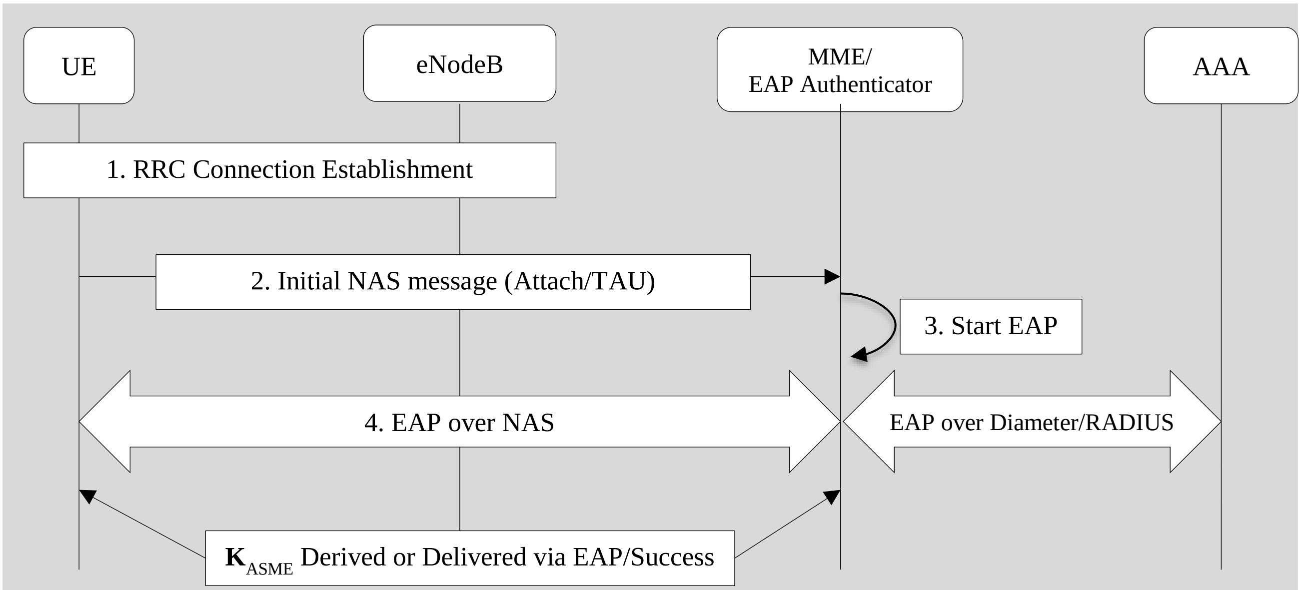


Figure 1 - Overview of EAP-Based Authentication Procedure Message Flow

1. The UE establishes an RRC connection with the eNodeB (or the eNB in 3GPP-based Access Mode).
2. The UE sends an Initial NAS message (e.g. Attach/TAU Request) to the NH-MME (for NHN Access Mode) or to the SP MME' (for 3GPP-based Access Mode (non-EPS-AKA)).
    a. The attach procedure continues as identified in 3GPP TS 23.401 Section 5.3.2.1[16] up to (and including) the Identity Response from the UE.
3. The local MME (NH-MME or SP MME') initiates the EAP authentication process
    a. When in NHN Access Mode, the NH-MME notifies the EAP authenticator function (which may be collocated with the NH-MME) to initiate EAP authentication.
    b. When in 3GPP-based Access Mode (non-EPS- AKA), the SP MME' notifies the EAP authenticator function (which may be collocated with the MME') to initiate the EAP authentication based on the UE-provided IMSI value (i.e., the 3GPP-based Access Mode is selected if the presented IMSI is configured for extended authentication on the SP MME').
4. The EAP authentication takes place over the NAS transport in both NHN and 3GPP-based Access Modes. In particular:

a. In NHN Access Mode, the identity used by the UE in response to the EAP Identity Request packet is provided in the Network Access Identifier (NAI) form in the EAP payload sent by the UE. The EAP packets exchange continues between the SP's non-3GPP AAA server through the Local AAA Proxy.

b. In 3GPP-based Access Mode (non-EPS-AKA), the identity used by the UE in response to the EAP Identity Request packet is provided in the IMSI form in the EAP payload sent by the UE. The EAP packets exchange continues between the SP's non-3GPP AAA server and the SP MME'.

Upon successful authentication, the UE and the NH-MME (for NHN Access Mode) or the SP MME' (for 3GPP-based Access Mode) derive the K_{ASME} from the EAP keying material (MSK) as defined in Section 5.12.4 of MFA MF.202 TS [6]. In particular, the K_{ASME} is defined as the 256 MSB (i.e., 32 Bytes) of the MSK that is generated as part of the EAP authentication method (e.g., TLS) by the UE and the AAA server.

After this point the MME (NH-MME for NHN Access Mode or SP MME' for 3GPP-based Access Mode) indicates to the UE that the NAS security is activated by sending a Security Mode Command (SMC) to the UE. The MME continues the NAS procedure. For example, for attach procedure Steps 17 to 24 as listed in Section 5.3.2.1 of 3GPP TS 23.401 [16] are performed.

4.2 Non-Certificate-Based Subscriber Authentication

SPs can support subscriber authentication methods that use credentials other than EPS-AKA and X.509 Certificates. In this case, SPs can support the EAP-TTLS method as described in the rest of this section, and other methods.

EAP-TTLS comprises two phases: the TLS handshake phase (also called phase 1) and the TLS tunnel phase (also called phase 2).

During phase 1, TLS is used to authenticate the TTLS server and, optionally, the client to the server via optional client certificates request. During this phase, the selection of a cipher suite and its activation allows for the next phase to proceed securely by using the TLS record layer.

During phase 2, the information exchanged between the client and the server (e.g., user authentication) is exchanged via either Diameter Attribute-Value Pairs (AVPs) or RADIUS Attributes that are encrypted by using the cipher selected during the TLS negotiation.

4.3 Certificate Based Subscriber authentication (CBSA)

Certificate Based Subscriber authentication (CBSA) and key agreement can be performed using the Extensible Authentication Protocol (EAP) RFC 5247 [15]. In particular, the EAP-TLS method can be used when the UE is already provisioned with a valid X.509 certificate for the subscriber.

5 AAA servers

5.1 AAA servers for NHN Access Mode

When NHN Access Mode is selected with extended subscriber authentication mechanism, the NH-MME interacts with the home SP's non-3GPP AAA Server via the Local AAA Proxy server when authenticating subscribers. In particular, since NHN Access Mode uses EAP authentication (instead of EPS-AKA):

- EAP packets are transported between the UE and the NH-MME by using extended NAS messages as defined in MFA TS 24.301 [32] Section 8.2.32MF1 and Section 8.2.32MF2.
- EAP packets are transported from NH-MME to EAP Authenticator, then Local AAA Proxy, and finally the SP's non-3GPP AAA. The interfaces between (a) the EAP Authenticator and the local AAA, and (b) the Local AAA Proxy and the non-3GPP AAA are based on Diameter (see RFC 6733 [34] and RFC 7075 [35]) or RADIUS (see RFC 3579 [33]). It follows the specifications for the SWa interface for Untrusted Access Mode and STa interface for Trusted Access Mode, as defined in 3GPP TS 29.273 [22].
- During the extended authentication procedures (i.e., in response to the *EAP-REQ/Identity* packet issued by the NH-MME), the UE indicates its home SP by providing its identity and home SP domain in a form of NAI defined in RFC 7542 [36]. The realm portion of the NAI is used by the Local AAA Proxy to route the EAP packets to the appropriate non-3GPP AAA Server.

5.2 AAA servers for 3GPP-based Access Mode (non-EPS-AKA)

When 3GPP-based Access Mode (non-EPS-AKA) is selected, the MME' interacts with the local non-3GPP AAA Server directly when authenticating subscribers. In particular, since this Access Mode uses EAP authentication (instead of EPS-AKA):

- EAP packets are transported between the UE and the MME' by using extended NAS messages as defined in MFA TS 24.301 [32] Section 8.2.32MF1 and Section 8.2.32MF2.
- EAP packets are transported from MME' to EAP Authenticator, and finally the Local non-3GPP AAA. The interfaces between the EAP Authenticator and the Local non-3GPP AAA are based on Diameter (see RFC 6733 [34] and RFC 7075 [35]) or RADIUS (see RFC 3579 [33]).

It is required that each non-USIM credential is associated with a unique IMSI value that the device must use in all authentication and identity procedures. In particular, during the attach, authentication, and identity request procedures, the UE shall provide its identity by using the IMSI associated with the subscriber's credentials used for authentication.

6 Extended Subscriber Authentication Specifications

This section provides the specifications for using Extended Subscriber Authentication (EAP-based) for NHN Access Mode and 3GPP-based Access Mode (non-EPS-AKA).

AAAs that support Extended Subscriber Authentication shall support EAP-TTLS/MSCHAPv2 and EAP-TLS methods and may support additional EAP methods with security level equal or higher than these methods.

UEs that support Extended Subscriber Authentication shall support EAP-TTLS/ MSCHAPv2 and EAP-TLS and may support additional EAP methods with security level equal or higher than these methods.

Operators that decide to support Extended Subscriber Authentication may use one of the secure EAP authentication methods supported by equipment providers (UE and AAA manufacturers). The supported EAP mechanisms shall have similar or higher security level than EAP-TTLS/MSCHAPv2 and EAP-TLS methods to prevent granting any advantage to the attacker.

EAP Tunneling methods shall be used to protect the confidentiality and integrity and shared secret data when extended authentication methods (non-Certificate-Based) are used.

6.1 TLS Parameters Selection for EAP methods

Both EAP-TTLS and EAP-TLS use the TLS protocol in order to establish a secure and authenticated communication channel between the UE and the AAA Server. SPs and UEs that support extended subscriber authentication shall use the following settings for the TLS negotiation for both EAP-TTLS[1] and EAP-TLS mechanisms, in particular:

- The TLS endpoints shall support TLS version 1.2 [27]. AAA server shall support the following ciphers and shall pick the first one (from the top of the following ordered list) that is supported by the UE during TLS negotiation:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

6.2 Extended Subscriber Authentication via EAP-TTLS

The EAP-TTLS [8] with MS-CHAP-V2 (defined in RFC 2759 [10]) authentication comprises two different phases.

During Phase One, the UE and the AAA server establish a secure communication channel by performing a TLS negotiation.

[1] As described in RFC 5281 Section 7.7.

During Phase Two, the subscriber's credentials are exchanged and verified. The data exchanged between the UE and the AAA Server is sent by using Diameter Attribute-Value Pairs (AVPs) or RADIUS Attributes: both parties are required to encode the information in a sequence of AVPs or Attributes that must be processed by the TLS record layer for encryption to ensure that the identity and credentials information exchanged within the tunnel is kept secure.

6.2.1 Phase One Call Flow

The call flow for Phase One of the initial attach procedure is depicted in Figure 2:

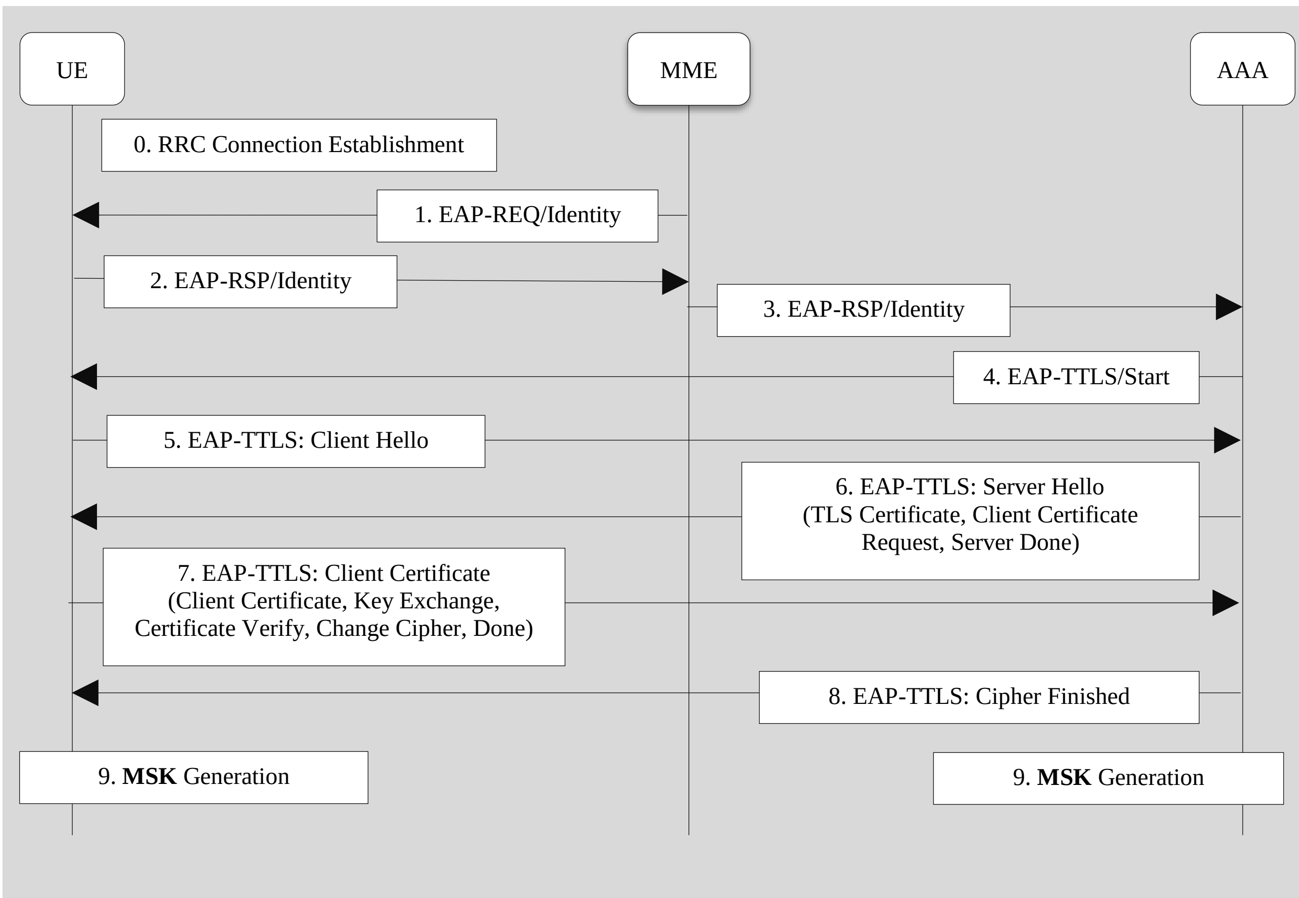


Figure 2 - Phase-one call flow for initial attach with EAP-TTLS

The call flow for Phase One is as follows:

1. After the initial RRC Connection Establishment, the MME (when in NHN Access Mode) or the SP MME' (when in 3GPP-based Access Mode [non-EPS-AKA]) initiates the EAP authentication procedure by sending the *EAP-REQ/Identity* packet to the UE.

2. The UE replies to the *EAP-REQ/Identity* with an *EAP-RSP/Identity* packet as described in Section 5.1 or 5.2 for NHN Access Mode and 3GPP-based Access Mode (non-EPS-AKA) respectively.
    - When in NHN Access Mode, the NH-MME uses the reported identity inside the *EAP-RSP/Identity* packet to route the packets to the appropriate AAA server via the Local AAA Proxy.
    - When in 3GPP-based Access Mode (non-EPS-AKA), the SP MME' uses the reported identity inside the *EAP-RSP/Identity* packet as the identity used in any subsequent procedure. Additionally, the MME' may decide to verify (depending on the SP's configured policy) that the presented identity is the same as the one used in the Identity Response and may decide to end the authentication procedure (i.e., fail) when the two values do not match.
3. The *EAP-RSP/Identity* packet is forwarded to the appropriate AAA Server where the *EAP-TTLS* authentication method for the presented identity is selected.
4. The AAA Server starts the selected EAP authentication mechanism by sending the *EAP-TTLS/Start* packet to the UE by setting the S (Start) bit in the packet as defined by RFC 5281 [8].
5. The UE starts the creation of the TLS tunnel by sending the *EAP-TTLS: Client Hello* packet to the AAA server with the initial parameters for TLS version selection and the supported list of ciphers.
6. The AAA server sends back the selected TLS version and selected cipher together with its own certificate (and certificate chain) in the *EAP-TTLS: Server Hello* packet. In addition, the server may include the request for an optional client certificate that may be used for device authentication during the establishment of the TLS channel.
    - This is a change in respect to Step 9 as defined in Section 5.12.3.4 of MFA MF.202 [6]. In particular, this step is modified in order to make client authentication during the TLS messages exchange optional as defined in RFC 5281 [8]. In case the UE has been provisioned with a device certificate, the UE shall include it in the Client Certificate response to the *Server Hello* message if the AAA Server included the request for client authentication.
7. The UE, after validating the server's certificate and certificate chain, replies to the *EAP-TTLS: Server Hello* packet by providing the selected cryptographic parameters (e.g., Client key exchange, Change Cipher, etc.) and, optionally, its own device certificate and the associated certificate chain.
    - If the UE has been provided with a unique device certificate and the server included the request for client authentication in the *Server Hello* message, the certificate shall be included in the EAP-RSP/EAP-TTLS that is transported to the MME over NAS

and then forwarded to the home SP's non-3GPP AAA Server via the Local AAA Proxy.

8. The AAA server proceeds with the validation of the client certificate (if provided by the UE) and sends the final packet to the UE with the indication of the successful TLS negotiation and final cipher selection.
    - If the UE does not provide a device certificate (i.e., in case an empty Client Certificate is sent in the response packet to the *Server Hello*), the home SP's non-3GPP AAA Server shall not declare EAP failure and shall not attempt to validate the client certificate in that case.
    - If a client certificate is provided by the UE, the AAA server shall attempt to validate it and, depending on the configured SP's authentication policy, the AAA server may decide to fail the authentication procedure if the client certificate is not trusted.
9. The Master Session Key (MSK) and the Extended Master Session Key (EMSK) keying material are generated based on secret information developed during the TLS handshake between client and TTLS server as described in Section 8 of RFC 5281 [8].
    - The first 256 MSB (32 Bytes) of the MSK are used as the K_{ASME} to protect the communication layer at the end of the authentication procedure as described in 6.2.2 and in Section 5.12.4 of MFA MF.202 [6].

At this point, Phase One of the EAP-TTLS is successfully completed and the process continues with the inner EAP authentication mechanism for the subscriber's credentials.

6.2.2 Phase Two Call Flow

Phase Two is about authenticating the credentials associated with the identity reported by the UE in the initial *EAP-RSP/Identity* packet.

The complete call flow for Phase Two is depicted in Figure 3:

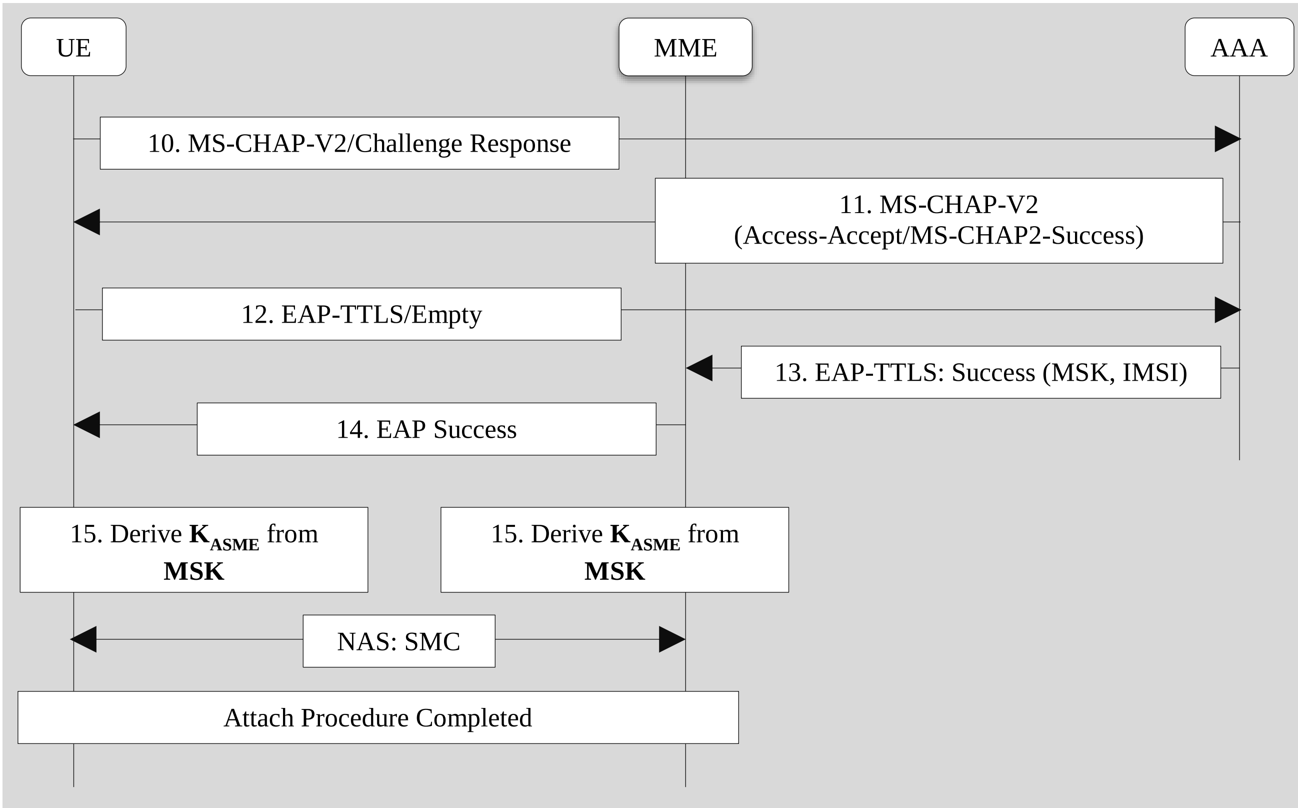


Figure 3 - Phase Two call flow for initial attach with EAP-TTLS

The call flow for Phase Two is as follows:

10. The UE initiates the subscriber's credentials authentication by sending the initial *MS-CHAP-V2/Challenge Response* packet as described in Section 11.2.4 of RFC 5281 [8]. In particular, the packet sent to the AAA server includes the *User-Name*, the *MS-CHAP-Challenge*, and the *MS-CHAP2-Response* AVPs.

    - The *subscriber credential* shall be the *User-Name* and associated secret (password) used in the MS-CHAP-V2/Challenge Response.

    - The *MS-CHAP-Challenge* value is taken from the challenge material generated on the UE (17 Bytes).

- The *MS-CHAP2-Response* consists of Ident (1 Byte from the challenge material), Flags (set to 0), Peer-Challenge (random value), and the Response (computed according to the MS-CHAP-V2 algorithm).

11. The AAA Server first verifies that the value of the *MS-CHAP-Challenge AVP* and the value on the Ident in the client's *MS-CHAP2-Response AVP* are equal to the values generated as challenge material. If the authentication is successful, the AAA Server will respond with an *MS-CHAP2-Access-Accept AVP* with the *MS-CHAP2-Success AVP* (a 42-octet string that authenticates the AAA Server to the UE).

    - At this point, the authentication is not yet complete as the UE must still accept the authentication response of the AAA Server.

12. The UE authenticates the server based on the *MS-CHAP2-Success AVP* and the *MS-CHAP-Challenge AVP* generated in step 10. If the authentication succeeds, the UE sends an *EAP-TTLS/Empty* packet to the AAA server containing no data (that is, with a zero-length Data field).

13. Upon receipt of the empty *EAP-TTLS/Empty* packet from the UE, the AAA server considers the MS-CHAP-V2 authentication to have succeeded and issues an *EAP-TTLS/Success* packet to the MME which carries the MSK that was derived during Phase One and the IMSI value associated with the credentials used for subscriber authentication.

    - The *MPPE-Recv-Key* and *MPPE-Send-Key* attributes defined in RFC 2548 [40] are used to distribute the first 32 octets and second 32 octets of the MSK, respectively.

    - The *Extended-Type-1* attribute defined in RFC 6929 [41] is used to distribute the IMSI value associated to the credentials used for subscriber authentication.

14. The MME notifies the UE that the subscriber authentication was successful by sending an *EAP-TTLS/Success* packet to the UE.

    - The *EAP-TTLS/Success* packet exchanged between the MME and the UE does not contain the MSK nor the authenticated IMSI value as the communication between the two parties is not yet secured. Moreover, the UE has already derived the MSK from Phase One and, therefore, the MSK does not need to be sent to the UE.

At this point the authentication is successfully completed.

6.2.3 EAP-TTLS Deployment for NHN Access Mode

The EAP authentication call flow shall follow the procedures described in the Section 6.2 with the following modifications:

- The AAA Server in Sections 6.2.1 and 6.2.2 is the SP's non-3GPP AAA Server.
- TLS cryptographic parameters shall follow the prescriptions in Section 6.1.

6.2.4 EAP-TTLS Deployment for 3GPP-based Access Mode (non-EPS-AKA)

The EAP authentication call flow shall follow the procedures described in the Section 6.2 with the following further modifications:

- The AAA Server in Sections 6.2.1 and 6.2.2 is the local SP's non-3GPP AAA Server.
- TLS cryptographic parameters shall follow the prescriptions in Section 6.1.

In order to prevent the UE from using subscriber credentials that are different from the identity provided in response to the first *EAP-REQ/Identity* packet from the MME', the use of EAP-REQ/Identity and *EAP-RSP/Identity* packets is prohibited after the successful completion of Phase One.

When anonymous subscriber identities are used in the initial *EAP-RSP/Identity* packet from the UE as described in Section 2.1.4 of RFC 5216 [5], the AAA server must communicate the value of the IMSI associated with the credentials used for subscriber authentication to the MME' by including it in the *EAP-TLS/Success* packet via the *Extended-Type-1* AVP as defined in Section 3.1 of RFC 6929 [41].

The MME' shall use the reported value for any subsequent operation involving the subscriber's identity (IMSI) and may decide to reject the connection in case the value reported by the AAA server does not match the value used in the initial Identity Request packet from Step 4 in Section 5.3.2.1 3GPP 23.401 [16].

6.3 Extended Subscriber authentication via EAP-TLS

The complete Message Flow for EAP-TLS [5] is depicted in Figure 4:

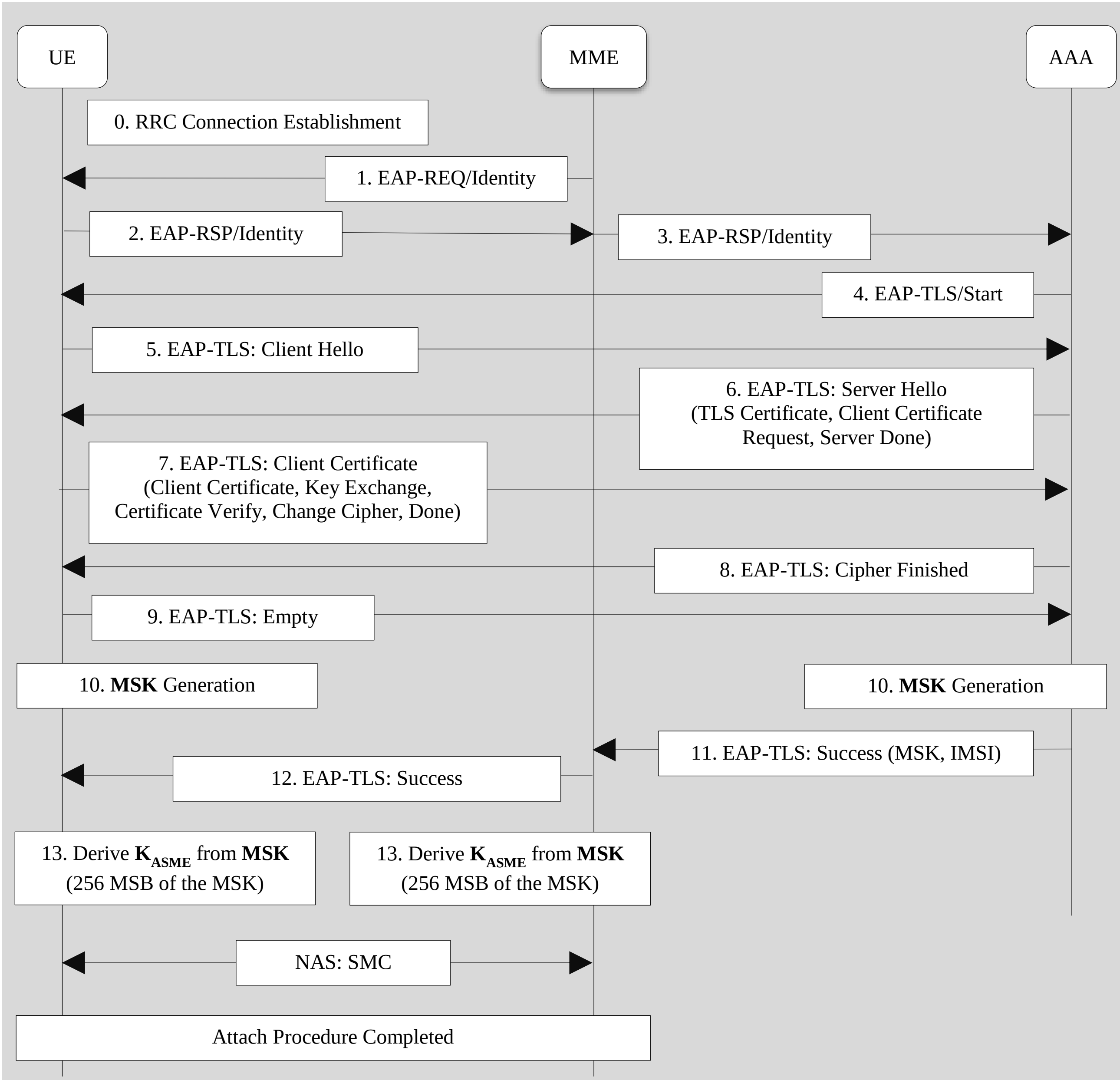


Figure 4 - Complete call flow for initial attach with EAP-TLS

The EAP authentication shall follow the procedures described in Section 5.12.3.3 of MFA TS MF.202 [6] and support the modifications described in this section. In particular, the following messages shall be used:

1. After the initial RRC Connection Establishment the MME (when in NHN Access Mode) or the SP MME' (when in 3GPP-based Access Mode [non-EPS-AKA]) initiates the EAP authentication procedure by sending the *EAP-REQ/Identity* packet to the UE.
2. The UE replies to the EAP-REQ/Identity with an *EAP-RSP/Identity* packet as described in Section 5.1 or 5.2 for NHN Access Mode and 3GPP-based Access Mode (non-EPS-AKA) respectively.
    - When in NHN Access Mode, the NH-MME uses the reported identity inside the *EAP-RSP/Identity* packet to route the packets to the appropriate AAA server via the Local AAA Proxy.
    - When in 3GPP-based Access Mode (non-EPS-AKA), the SP MME' uses the reported identity inside the *EAP-RSP/Identity* packet as the identity used in any subsequent procedure. Additionally, the MME' may decide to verify (depending on the SP's configured policy) that the presented identity is the same as the one used in the Identity Response and may decide to end the authentication procedure (i.e., fail) when the two values do not match.
3. The *EAP-RSP/Identity* packet is forwarded to the appropriate AAA Server where the EAP-TLS authentication method for the presented identity is selected.
4. The AAA Server starts the selected EAP authentication mechanism by sending the *EAP-REQ/EAP-TLS: Start* packet to the UE by setting the S (Start) bit in the packet as defined by RFC 5216 [5].
5. The UE starts the creation of the TLS tunnel by sending the *EAP-RSP/EAP-TLS: Client Hello* packet to the AAA server with the initial parameters for TLS version selection and the supported list of ciphers.
6. The AAA server sends back the selected TLS version and selected cipher together with its own certificate (and certificate chain) in the EAP-REQ/*EAP-TLS: Server Hello* packet. In addition, the server includes the request for mandatory client certificate that will be used for subscriber authentication (mutual authentication).
7. The UE, after validating the server's certificate and certificate chain, replies to the EAP-RSP/*EAP-TLS: Server Hello* packet by providing the selected cryptographic parameters (e.g., Client key exchange, Change Cipher, etc.) together with the subscriber certificate and the associated certificate chain.
8. The AAA server proceeds with the validation of the client certificate and sends the final packet to the UE with the indication of the successful TLS negotiation and final cipher selection.
    - If the UE does not provide a device certificate, then the home SP's non-3GPP AAA Server must fail the EAP authentication unless the server will request the certificate

after the TLS finished message to protect the subscriber's identity as described in 6.3.1 and 6.3.2.

- If the UE provides a device certificate, the AAA server must attempt to validate the subscriber's certificate and shall fail in case the validation of the certificate shall fail for any reason.

9. The UE sends an *EAP-TLS/Empty* packet to the AAA server containing no data (that is, with a zero-length Data field) indicating the completion of the TLS negotiation.
10. On both the UE and the AAA server, the Master Session Key (MSK) and the Extended Master Session Key (EMSK) keying material is generated based on secret information developed during the TLS handshake between client and TLS server as described in Section 8 of RFC 5281 [8].
11. Upon receipt of the empty *EAP-TLS/Empty* packet from the UE, the AAA server considers the EAP-TLS authentication to have succeeded and sends an *EAP-TLS/Success* packet to the MME which carries the MSK that was derived during Phase One and the IMSI value associated with the credentials used for subscriber authentication.
    - The *MPPE-Recv-Key* and *MPPE-Send-Key* attributes defined in RFC 2548 [40] are used to distribute the first 32 octets and second 32 octets of the MSK, respectively.
    - The *Extended-Type-1* attribute defined in RFC 6929 [41] is used to distribute the IMSI value associated with the credentials used for subscriber authentication.
12. The MME notifies the UE that the subscriber authentication was successful by sending the *EAP-TTLS/Success* packet to the UE.
    - The *EAP-TTLS/Success* packet exchanged between the MME and the UE does not contain the MSK nor the authenticated IMSI value as the communication between the two parties is not yet secured. Moreover, the UE has already derived the MSK from Phase One and, therefore, the MSK does not need to be sent to the UE.
13. On both the UE and the MME, the first 256 MSB (32 Bytes) of the MSK are utilized as the K_{ASME} that is used to protect the communication layer at the end of the authentication procedure as described in Section 5.12.4 of MFA MF.202 [6].

At this point the EAP-TLS is successfully completed.

6.3.1 EAP-TLS Deployment for NHN Access Mode

The EAP authentication call flow shall follow the procedures described in the Section 6.3 and in Section 5.12.3.3 of MFA TS MF.202 [6] with the following modifications:

- The MME in Section 6.3 is the NH-MME.

- The AAA Server in Section 6.3 is the local SP's non-3GPP AAA Server.
- TLS cryptographic parameters shall follow the prescriptions in Section 6.1.

As discussed in Section 5.12.3.3 of MFA MF.202 [6], the user identity may be protected as described in Section 2.1.4 of RFC 5216 [5]. In this case the actual identity is retrieved from the Client certificate that shall be sent after Step 8 (TLS Finished), i.e. under the TLS protection. In particular, the SP's non-3GPP AAA server continues the TLS handshake requesting the Client certificate again after Step 8 and performs the client certificate validation before sending the final *EAP-TLS/Success* packet.

In this case, the AAA may include the value of the IMSI associated with the credentials used for subscriber authentication in the *EAP-TLS/Success* packet via the *Extended-Type-1* AVP as defined in Section 3.1 of RFC 6929 [41].

6.3.2 EAP-TLS Deployment for 3GPP-based Access Mode (non-EPS-AKA)

The authentication flow is the same as depicted in 3GPP 23.401 Section 5.3.2 [16] up to, but excluding, 5a. In particular the User Authentication Request and the User Authentication Response messages are replaced by the call flow described in Section 6.3.

The EAP authentication call flow shall follow the procedures described in the Section 6.3 and in Section 5.12.3.3 of MFA TS MF.202 [6] with the following modifications:

- The MME in Section 6.3 is the SP MME'.
- The AAA Server in Section 6.3 is the local SP's non-3GPP AAA Server.
- TLS supported parameters shall follow the prescriptions in Section 6.1.

In this Access Mode, the use of anonymous identities in the *EAP-RSP/Identity* packet from the UE in Step 2 as described in Section 2.1.4 of RFC 5216 [5] may be supported by the SP MME' during the initial attach procedure. In this case, the AAA server must communicate the value of the IMSI associated with the credentials used for subscriber authentication to the MME' by including it in the *EAP-TLS/Success* packet via the *Extended-Type-1* attribute as defined in Section 3.1 of RFC 6929 [41].

When real identities are used in the *EAP-RSP/Identity* packet from the UE, in order to make sure that the identity reported during the attach procedure is the actual one used during the authentication process, the AAA server must verify that the identity used in the *EAP-RSP/Identity* packet is the same as the one that is presented in the client certificate used for subscriber authentication. Also in this case, the AAA shall include the value of the IMSI associated with the credentials used for subscriber authentication in the *EAP-TLS/Success* packet by using the *Extended-Type-1* attribute as defined in Section 3.1 of RFC 6929 [41].

APPENDICES

A (Informative): Trust Management

This Annex provide guidelines for the deployment of trust infrastructures that can be used for both UEs and the authentication infrastructure (i.e., AAA and OSU servers). Moreover, this Annex also considers the impact of deploying Online Sign Up (OSU) services to provide certificate-based credentials to UEs.

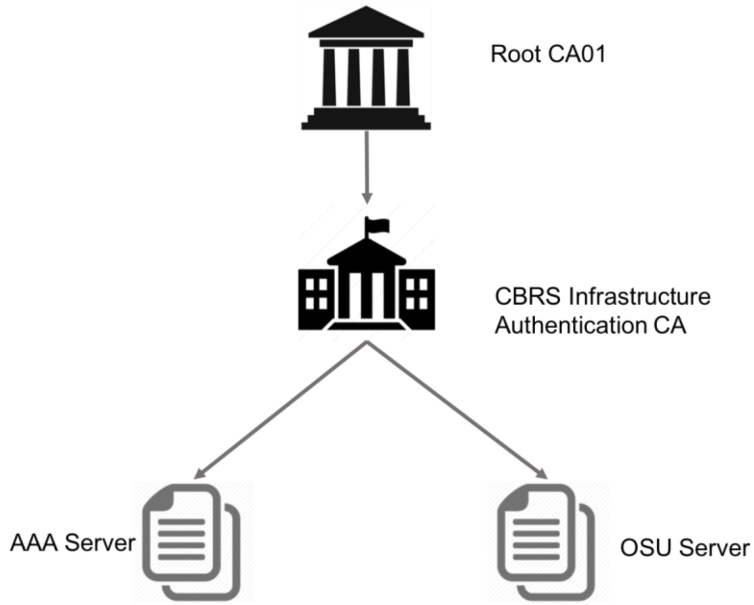
A.1 Centralized vs. Distributed PKIs

There are two main PKI models that operators can adopt. The first one is a centralized model where certificates are issued within a common PKI. This model allows the operator to have full control over the structure of the PKI and the certificate profiles.

The second model is a distributed model where participating operators use a common PKI (i.e., a common Root CA) where each operator will be able to obtain and operate its own Intermediate CA. This model allows the possibility to use a single Trust Anchor in UEs to validate the authentication infrastructure's credentials by using a single Trust Anchor.

> NOTE: In this section, the term "CBRS Infrastructure Authentication CA" is used in a generic sense and refers to a generic (non CBRS operated) Certification Authority that issues certificates to be used in the CBRS context.

The following figure provides a minimum viable PKI for providing certificates for the authentication infrastructure (i.e., server-side authentication):



In this model, the AAA Server Certificate is used to authenticate the AAA server to the UE during the extended authentication (i.e., EAP-TTLS and EAP-TLS methods) while the OSU Server Certificate is used to authenticate the OSU server during the UE registration process (i.e., during the TLS session establishment when the UE connects to the OSU server).

Once established, this PKI can also be used to provision subscribers' certificate to UEs via the OSU server (if supported) or via other out-of-band mechanisms.

A.2 Restricting Trust to a specific branch of a PKI

Sometimes PKIs can have complex connections and multiple SubCAs dedicated to specific use. It is common practice, for example, to have, in the same infrastructure, a single Trust Anchor that issues "scoped" SubCAs (e.g., a Device SubCA, a Server SubCA, and a Code Signing SubCA).

SPs can decide to restrict trust for subscribers' authentication to a specific subset of the SubCAs issued under a Trust Anchor (i.e., only certificates issued by the identified SubCAs can be used for CBSA).

In order to accommodate this requirement, the SP must, after verifying that the certificate chains up to one of the installed Trust Anchors (i.e., the Root CA), verify that the Issuer of the certificate to be validated during the EAP-TLS session is the one (or one of the allowed ones) the SP wants to restrict the trust to by checking that the Issuer of the subscriber's certificate is in the allowed set.

A.3 Internal vs. External X.509 Certificate Validation

One of the key aspects of CBSA is the provisioning and management of X.509 certificates for the UE. Some SP might decide not to offer certificate provisioning for UE (i.e., they will not directly issue certificates for their subscribers), and still want to leverage CBSA to extend the range of services offered to their customers.

In this case, SPs might decide to accept certificates issued and provisioned by third parties. For example, this could include certificates issued to the UE in the context of WiFi registration or certificates issued on behalf of the SP by a Certificate Service Provider.

Whatever the choice by the SP might be, by using CBSA, the SP has the ability to combine all the above options by simply adding the required Trust Anchors (i.e., Root CAs certificates or Public Keys) to the list of trusted authorities in the SP's AAA infrastructure without requiring the sharing of credentials' databases with the third parties that provide and manage the UE's certificates.

A.4 Direct and Indirect Server Authentication

When EAP-AKA'[4] is used for subscriber authentication, the identity of the server is indirectly verified during the authentication process by ensuring that the server is using the same shared key as the one stored inside the USIM. In this case, the provisioning of the trusted secret key for authentication is achieved via the provisioning of the USIM that serves as the base of trust for the UE.

On the contrary, when EAP-TLS or EAP-TTLS methods are used for subscriber authentication, the UE is required to directly authenticate the AAA Server by verifying that the server's certificate is trusted, not expired, and not revoked. In particular, for the UE to be able to verify the server's certificate, the Trust Anchor that provides the root of trust for the server's certificate must be securely stored in the UE. This trust anchor is usually installed together with the UE credentials during the subscriber's registration process.

A.5 UE Subscriber Certificate Provisioning for EAP-TLS

The provision of UE certificates can happen through different processes and protocols: out-of-band or online (in-band) mechanisms. The out-of-band provisioning case (e.g., via a web portal or via pre-installed credentials in USIM), is not covered in this document.

For the second case, i.e. online provisioning, the operator may decide to support certificate provisioning and installation procedures as described in Section 5.14 of MFA [6] by deploying support for an Online Sign Up (OSU) server or other mechanisms (e.g., via the EAP protocol itself).

A.5.1 Network Impact and Security Considerations for OSU deployment

In case the operator decides to deploy support for OSU, the operator shall follow the procedures for on-boarding new clients as described in Section 5.14 of [6]. In this case, section 5.5.2.1 of TS 1002 [3] is modified to include support for Online Sign-up (OSU). In particular, the deployment of the OSU server adds several requirements from a network perspective and introduces important security requirements that the SP must take into serious consideration.

In particular, the deployment of the OSU component requires the following changes in the SP's CBRS network:

Support for the OSU must be broadcasted by the network. In particular, the OSU support information is delivered to the UE by using SDP Query for OSU information as described in Section 5.10.7 of MFA [6].

The UE shall request a PDN connection for a default Access Point Name (APN) after indicating its intention to engage with the OSU process by using an OSU-specific Attach Type.

The network operator shall support the UE to enter a sub-state of the EMM-REGISTERED that provide a PDN connection restricted to provisioning a specific (set of) OSU server(s) and does not grant access to normal service.

Depending on the type of credentials that were provisioned during the onboarding process, the OSU AAA server must be able to update the SP's AAA server with the new credentials

A.6 Considerations about Manufacturer (or Device) Certificates

When using extended authentication, the use of a device certificate is suggested to provide client-side authentication in the EAP-TTLS case. The manufacturer certificate is used to convey some important parameters that may be included also in the Subscriber's certificate profile in case the operator wants to tie the subscription to a specific device.

NOTE: It is important to understand that the manufacturer (or device) certificate is not related to the user subscription, but it is a device-specific identity only.

The provisioning mechanism of this type of certificate is not specified in this document. In particular, it is assumed that the device is pre-installed with the manufacturer (or device) certificate (and the corresponding private key) by the manufacturer in a secure fashion. In the manufacturer certificate, the following information may be present:

- IMEI (OID 1.3.6.1.4.1.40808.1.1.3)
- MEID (OID 1.3.6.1.4.1.40808.1.1.4)
- DEVID (OID 1.3.6.1.4.1.40808.1.1.5)

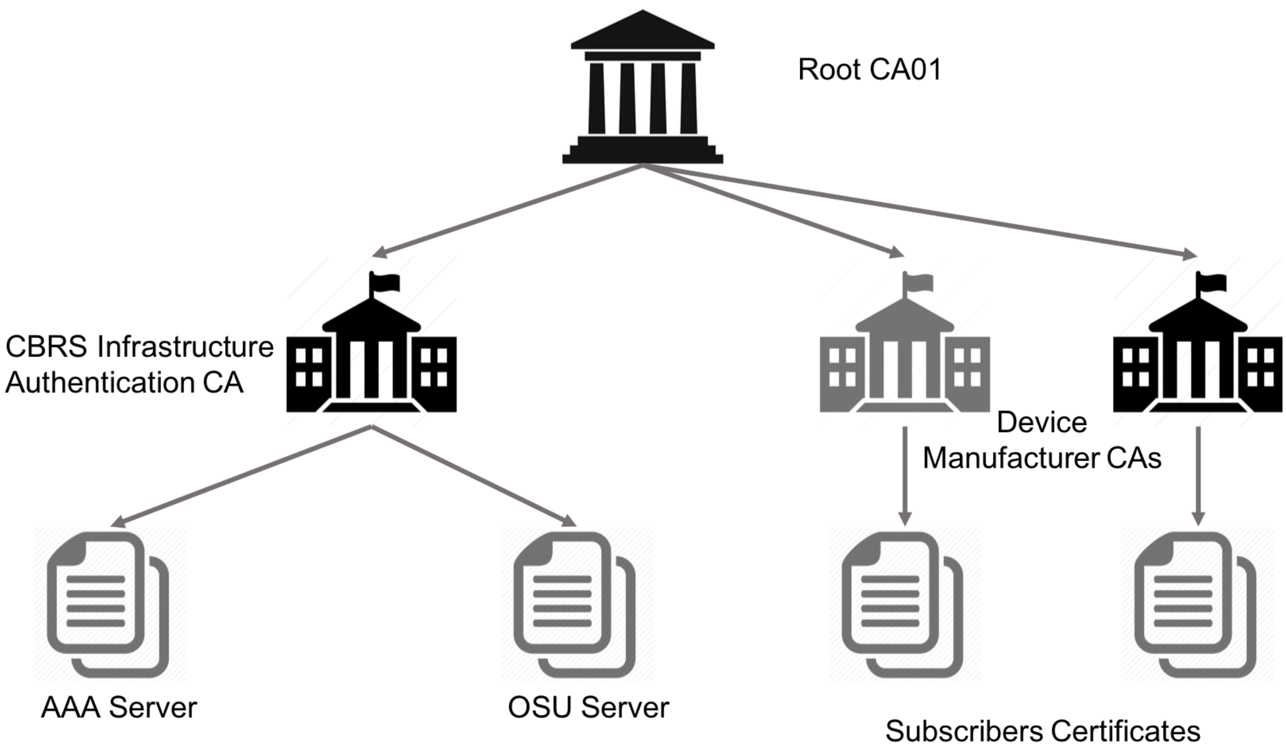
Optionally, the following information may be present:

- MACADDRESS (OID 1.3.6.1.1.1.1.22)

In order to foster interoperability across manufacturers, operators might decide to provide the possibility to issue a manufacturer's CA certificate for approved devices under a common PKI or under a specific operator PKI. Additionally, operators might decide to include the manufacturer's Root CA into their authentication servers (e.g., OSU and AAA) to be able to correctly validate the device certificate when used.

It is suggested that manufacturers who would like to obtain a certificate from the common or operator-specific PKIs (i.e., for issuing certificates for its own devices) shall pass an audit against the Certificate

Policy that applies to the specific PKI. The following Figure depicts an extended model for the PKI which includes the Device Manufacturers' Intermediate Certification Authorities:



A.6.1 User Equipment Trust Anchors Installation

In order for the UE to be able to verify the authentication infrastructure, UEs must be installed with the Root CA certificate (e.g., Root CA01). This allows the UE to verify that the chain of certificates presented during authentication by both the AAA server and the OSU server anchors to a trusted entity.

A.6.2 Authentication Infrastructure Trust Anchors Installation

In order for AAA and OSU servers to be able to verify the identity of devices (if manufacturer's certificates are installed on the UEs) or of subscribers (if EAP-TLS is used as the authentication mechanism), the Root CA certificates must be installed. If a common PKI is used for both subscribers and manufacturers, then only a single root is required to be installed on the server. In case different PKIs are used instead, all the Root CAs from different manufacturers are required on all servers.

A.7 Certificates Profiles

This section provides examples for the definition of the profile for the different types of certificates for the authentication infrastructure (i.e., AAA and OSU servers). The profile for subscriber certificates is left unspecified as this might vary greatly among providers.

Table 1 - CBRS Authentication Infrastructure – Root CA Certificate Profile

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		o=<organization name> ou=Root CA01 cn=CBRS Root Certification Authority		
Subject DN		o=<organization name> ou=Root CA01 cn=CBRS Root Certification Authority		
Validity Period		48 yrs		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Public Key		RSA 4096 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1

Attribute Name		Settings		
subjectAltName	{id-ce 17}	O	FALSE	
directoryName				Set by the issuing CA

Table 2 - CBRS Authentication Infrastructure – Intermediate CA Certificate Profile

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		o=<organization name> ou=Root CA01 cn=CBRS Root Certification Authority		
Subject DN		o=<organization name> ou=Infrastructure Authentication cn=Certification Authority 01		
Validity Period		Up to 16 yrs		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Public Key		RSA 4096 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	X	FALSE	

Attribute Name		Settings		
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1

Table 3 - CBRS Authentication Infrastructure – AAA Server Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		o=<organization name> ou=CBRS Infrastructure Authentication cn= Certification Authority 01		
Subject DN		o=<organization name> ou=CBRS Infrastructure Authentication ou=AAA Services cn=<server FQDN>		
Validity Period		Up to 4 yrs		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Public Key		RSA 2048 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	

Attribute Name		Settings		
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	X	FALSE	
dNSName				<server FQDN>

Table 4 CBRS Authentication Infrastructure – OSU Server Certificate

Attribute Name		Settings		
Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		o=<organization name> ou=CBRS Infrastructure Authentication cn= Certification Authority 01		
Subject DN		o=<organization name> ou=CBRS Infrastructure Authentication ou=OSU Services cn=<server FQDN>		
Validity Period		Up to 4 yrs		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Public Key		RSA 2048 bits		
Parameters		NULL		
Standard Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	{id-ce 35}	X	FALSE	

Attribute Name		Settings		
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	X	FALSE	
dNSName				<server FQDN >

All certificates issued under this PKI shall follow the procedure described in a Certificate Policy that governs the practices followed by the selected Certificate Service Provider

B (Informative): EAP Security Considerations

B.1 EAP-based Subscriber Authentication

CBRS supports extended authentication mechanisms for both NHN Access Mode and 3GPP-based Access Mode (non-EPS-AKA) via the EAP protocol. The use of EAP provides an extensible approach that allows to support multiple authentication methods without requiring modifications to the network architecture.

The selection of the EAP method used for subscriber authentication happens at the SP AAA server in response of the EAP-RSP/Identity initial authentication request packet [15]. With the introduction of additional methods and the possibility to support multiple types of credentials at once (e.g. some UE might support multiple mechanisms and/or might have multiple type of credentials that might be used for the same subscription – e.g., USIM-based and X.509 certificate), the selection of the appropriate authentication method might require some additional application logic on the SP's AAA (for NHN Access Mode) or on the SP MME' (for 3GPP-based Access Mode (non-EPS-AKA)).

In the most common case, the SP will be able to pre-select the authentication mechanism specific for that subscriber's device by maintaining the association between the subscriber's identity (e.g., IMSI or NAI) and the type of credentials that have been issued during the subscriber's registration process. Thus, in practice, when responding to the *EAP-RSP/Identity* packet, the SP AAA can still pre-select the appropriate EAP method directly without requiring the implementation of additional procedures. For example,

- If the subscriber registered its account with the SP by using username and password (e.g., via a web portal), the initial EAP response from the SP AAA server can use the EAP-TTLS [8] Start packet and the authentication will proceed by using MS-CHAP-V2 [10] as the inner method of the EAP-TTLS authentication.
- For a subscriber whose equipment was provisioned with an X.509 certificate during the registration process, the SP AAA server can use the EAP-TLS [5] Start packet instead.

- For USIM-based subscribers, the EAP-AKA’ can be selected as the authentication mechanisms as usual. Notice that other EAP methods can be selected in case the SP and the UE provide support for them.

B.2 EAP methods negotiation

In case multiple types of credentials are associated with a subscriber’s identity or if the EAP method selected by the SP is not supported by the UE, the UE can negotiate a different mechanism with the AAA server.

In particular, when the UE authenticates to the network and it does not support the EAP method pre-selected by the SP, the UE can follow the procedures described in RFC 3748 [26] to negotiate the appropriate EAP method that is supported.

It is important to notice that enabling negotiation of EAP methods might raise some security concerns. In particular, the negotiation process is vulnerable to downgrade attacks where an attacker with full network access can force the EAP endpoints to negotiate a less secure method.

B.3 EAP Tunneling mechanisms

Support for EAP Tunneling methods is required when extended authentication methods (non-Certificate-Based) are used to protect the integrity and secrecy of the secret password. There are several existing tunnel-based EAP methods that use Transport Layer Security (TLS) [27] to establish the secure tunnel. This specification defines the procedures to deploy EAP-TTLS method for providing EAP tunneling capabilities, however operators and equipment providers can support additional ones.

B.4 Security Considerations

An important deployment consideration about the use of CBSA is that since the subscriber’s secret (i.e., the private key) is never shared or stored in the SPs system, its use removes the threat of an attacker stealing the subscribers’ authentication credentials by attacking the SP’s servers. This differs from the case where EAP-TTLS or EAP-AKA’ are used since the use of symmetric secrets requires both parties to have access to them, thus requiring SPs to store the secrets in their systems.

B.4.1 Crypto Implementation Security

Although CBSA provides high level of security, it is important that the procedures for certificate validation and revocation processing are implemented according to standard specification and best practices. Moreover, SPs can use standard schemes and algorithms for certificates, public keys and certificate signing. It is suggested that SPs follow the Commercial National Security Algorithm Suite (CNSA Suite) in their implementation for their PKIs and crypto parameters wherever possible.

B.4.2 Credential Security

The use of EAP-TTLS allows for the UE to cryptographically verify the identity of the AAA server (direct verify) when the appropriate Trust Anchor is available in the UE. However, it is important to notice that the security of the subscriber's authentication is dependent on the quality of the secret selected (i.e., the password) during the subscriber's registration. The SP can follow best practices for password management are properly followed to provide an adequate level of security during the authentication process.

Another important consideration related to the use of username and password is the possibility for malicious actors to guess the user's credentials. Differently from the EAP-TLS case, the attacker might attempt to guess credentials by trying many different username and password combinations. SPs that support this authentication mechanism can mitigate this type of attack using methods such as throttling, disabling of a subscriber's account, etc.

As a mitigation for reducing these risks, SPs can also choose to require device authentication via the use of client-side X.509 certificates during the Phase One of EAP-TTLS authentication (i.e., during TLS tunnel establishment).

B.4.3 UE Credentials Storage

In order to avoid requiring a user to enter his or her credentials every time the UE is required to authenticate to the network (or in case the credentials are directly provisioned to the device without requiring the subscriber to directly provide them), the UE can store the credentials in a persistent secure storage. In particular, the UE can store the credentials securely on the device to prevent an attacker from impersonating the subscriber.

Although it is out of scope of this document to provide an indication to UE manufacturers about how to implement security mechanisms and controls to protect the subscriber's credentials, in case the UE is equipped with USIM, secure storage, secure elements (e.g., cryptography-capable hardware), or similar hardware-protected storage, it shall be possible for the UE to leverage these components to protect the subscriber credentials and relevant configuration options.

C (Informative): Change History

Table 5 - Change History

Document history			
Version	**Date**	**Description**	**Implemented CRs**
V1.0.0, Rev 4.3	2019/01/11	Reformatting headers, footers, and references to be consistent with TS-1002.	

V1.0.0, Rev 4.2	2018/12/14	Implemented comment resolutions from re-balloting process.	
V1.0.0, Rev 4.1	2018/10/31	Removed “Contributors”, fixed typos, fixed inconsistent use of lower and upper cases, and added missing section number.	
V1.0.0, Rev 4.0	2018/10/27	Implemented comment resolutions from the balloting process.	