**3GPP TSG-SA3 Meeting #104-e *S3-212564-r3***

**e-meeting, 16-27 August 2021**

**Source: CableLabs, Ericsson, Charter Communications, Intel**

**Title: Annex X on EAP\_TTLS for SNPN**

**Document for: Approval**

**Agenda Item: 4.17**

# 1 Decision/action requested

***It is proposed to approve the changes to the draft-CR for eNPN***

# 2 Rationale

This contribution proposes a solution based on EAP-TTLS for authenticating UE with an exteral entity, where the EAP-TTLS server runs on the home AAA server. This solution removes the impact on the AUSF by the EAP-TTLS server. Further, it is compatible with the existing deployment of EAP-TTLS in operator networks where the EAP-TTLS server runs on the AAA.

The benefits of using EAP-TTLS is two-fold. First, it allows UE to be authenticated by an external entity that uses both EAP and non-EAP based authention. Second, the MSK used to derive 5G keys is received from the home AAA that is located with the operator network, thus removing the threat of eavesdropping in the radio networks by an external party.

The trust anchor used to authenticate the EAP-TTLS server certificate can be easily obtained from an operator’s website (as it is done today by some operators) or via the initial provisioning procedure.

# 3 Detailed proposal

**\*\*\*\*START OF CHANGES \*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 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')".

[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 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[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] Void

[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".

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

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[xx] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)"

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

Annex X (Informative): Primary Authenitcation using EAP-TTLS in Standalone Non-Public Networks

#### X.1 Introduction

In SNPN, when a credential holder is located outside of the SNPN, EAP-TTLS can be used to authenticate the UE. EAP-TTLS consists of two phases of authentication. In the first phase, a TLS tunnel is established between the UE and the EAP-TTLS server on AUSF . In the second phase, a legacy authentication protocol can be run towards between the UE and the credential holder (namely AAA) through the established TLS tunnel.

After the successful completion of EAP-TTLS, the AUSF and the UE derive the KAUSF from the EMSK.

UE is provisioned with a trust anchor to enable verification of the EAP-TTLS server certificate. This trust anchor can be obtained by a UE via a resource locator or provisioned into the UE during an onboarding procedure, which is out of the scope of this procedure.

#### X.2 Procedure



Figure: X.2-1: Primary authentication with external domain

0. The UE is configured with the trust anchor needed to authenticate the certificate of the EAP-TTLS server running on the AUSF. Further, the UE is configured with the credentials to authenticate with the external AAA server.

1. The UE selects the SNPN and initiates UE registration in the SNPN including a SUCI/SUPI. The SUPI is on NAI format, e.g., username@realm.

For construction of the SUCI, existing methods in clause 6.12 can be used. If the public key of the SNPN is not provisioned in the UE, the "username" part must be either omitted or "anonymous".

2. The AMF/SEAF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [2].

3. The AUSF checks with UDM within the SNPN for the authentication method to be executed for the UE using a Nudm\_UEAuthentication\_Get service operation. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [2].

4. The UDM resolves the SUCI to the SUPI before checking the authentication method applicable for the UE. The UDM can obtain the common subscription data or individual subscription data based on the SUPI.   
  
The UDM determines that primary authentication is to be performed using EAP-TTLS based on subscription data or by interpreting the realm part of the NAI.

5. The UDM provides the AUSF with the UE SUPI and the applicable authentication method for the UE. In this case, the UDM indicates to the AUSF that the primary authentication using EAP-TTLS. The UDM provides the AUSF also with the address of the AAA if required for the second phase of EAP-TTLS authentication.

6.

6. The AUSF starts EAP-TTLS and sends to the AMF/SEAF a Nausf\_UEAuthentication\_Authenticate Response message containing an EAP-Request message of EAP-type=EAP-TTLS with the Start(S) bit set, denoted as EAP-Request [EAP-TTLS, Start=1].

7. The AMF/SEAF forwards to the UE the EAP-Request [EAP-TTLS, Start=1] in the Authentication Request message, including the ngKSI and the ABBA parameters.

8. The UE replies to the AMF/SEAF an Authentication Response message containing an EAP-Response [EAP-TTLS] message whose data field encapsulates a TLS ClientHello message, denoted as EAP-Response [EAP-TTLS, ClientHello].

9. The AMF/SEAF forwards to the AUSF the EAP-Response [EAP-TTLS, ClientHello] message in a Nausf\_UEAuthentication\_Authenticate Request message.

10. The AUSF replies to the AMF/SEAF with an EAP-Request [EAP-TTLS] message whose data field encapsulates a TLS ServerHello message, a TLS ServerCertificate message, a TLS ServerKeyExchange message, and a TLS ServerHelloDone message. Such EAP-Request message is denoted as EAP-Request [EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateRequest\*, ServerHelloDone], and is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

11. The AMF/SEAF forwards to the UE the EAP-Request [EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, ServerHelloDone] message in an Authentication Request message, including the ngKSI and the ABBA parameters.

12. The UE authenticates the AAA-H by validating the server certificate included in the EAP-Request message received in step 15. The UE needs to be provisioned with certificates of a trust anchor to validate the AAA-H server certificate.

13. If the TLS server authentication is successful, then the UE replies to the AMF/SEAF with EAP-Response [EAP-TTLS] in an Authentication Response message. The data field of the EAP-Response [EAP-TTLS] message contains a TLS ClientKeyExchange message, a TLS ChangeCipherSpec message, and a TLS Finished message. This EAP-Response message is denoted as EAP-Response [EAP-TTLS, ClientKeyExchange, ChangeCipherSpec, Finished].

14. The AMF/SEAF forwards to the AUSF the EAP-Response [EAP-TTLS, ClientKeyExchange, ChangeCipherSpec, Finished] message in a Nausf\_UEAuthentication\_Authenticate Request message.

15. The AUSF sends to the AMF/SEAF an EAP-Request [EAP-TTLS] message with its data field encapsulating a TLS ChangeCipherSpec message and a TLS Finished message. This EAP-Request message is denoted as the EAP-Request [EAP-TLS, ChangeCipherSpec Finished] and is encapsulated in a Nausf\_UEAuthentication\_Authenticate Response message.

16. The AMF/SEAF forwards to the UE EAP-Request [EAP-TLS, ChangeCipherSpec Finished] message in an Authentication Request message, including the ngKSI and the ABBA parameters. By this point, the UE and the AAA-H have successfully established a TLS tunnel to protect EAP-TTLS phase 2, as well as keying materials to be used to derive the MSK and EMSK.

17. The UE runs EAP-TTLS phase 2 authentication towards the AAA as specified in RFC 5281 [XX] via NSSAAF. The EAP-TTLS phase 2 is mutual authentication between the UE and the AAA.

Editor’s Note: the interface between the AUSF and the NSSAFF is Radius/Diameter over SBI, and the interface between the NSSAAF and AAA is Radius/Diameter. The details of phase 2 is FFS.

18. After the EAP-TTLS phase 2 authentication succeeds, the AUSF derives the KAUSF from the EMSK by using the 256 msb of the EMSK as KAUSF. The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6.

19. The AUSF sends an Nausf\_UEAuthentication\_Authenticate Response message to the AMF/SEAF including an EAP-Success message along with the SUPI and the KSEAF.

20. The AMF/SEAF forwards to the UE the EAP-Success message, ngKSI and ABBA in an Authentication Result message or a Security Mode Command message.

21. Upon receiving the EAP-Success message, the UE derives an EMSK from the keying materials obtained in EAP-TTLS phase 1. The UE further derives the KAUSF by using the 256 msb of the EMSK. The UE then derives the KSEAF as defined in Annex A.6.

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