**3GPP TSG-SA3 Meeting #101-e *S3-*** ***202888-r1***

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

**Source: CableLabs**

**Title: Updates to solution #3**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***It is proposed to approve the changes to solution #20 in TR 33.809.***

# 2 Rationale

This contribution updates solution #3 by providing call flows for EAP-TTLS phase 1 and correcting minor errors and inconsistency between the figure and the texts

# 3 Detailed proposal

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

#### 6.3.2.1 Procedure



Figure: 6.3.2-1: Primary authentication with external domain

0. The UE is configured with credentials from the CdP e.g. SUPI containing a network-specific identifier, and credentials for any key-generating EAP-method.

The UE and TTLS server (AUSF) may have a one-way security relationship based on the TTLS server's (AUSF) possession of a private key guaranteed by a CA certificate which the user trusts or may have a mutual security relationship based on certificates for both parties.

1. The UE selects the SNPN and initiates UE registration in the SNPN. The UE creates a SUCI/SUPI based on the CdP-UE ID provided by the CdP and provisioned in the UE.

NOTE 1: It is assumed that the SUPI is on NAI format and includes also the CdP ID in the domain part of the NAI, e.g. UEID@CdPID.

For construction of the SUCI, existing methods in TS 33.501 [2] can be used. If the public key of the SNPN is not provisioned in the UE, null scheme can be used with anonymised SUPI as described in Annex B of TS 33.501 [2].

Editor's note: User privacy for key-generating EAP-methods not covered by current procedures in TS 33.501 [2] is FFS.”

2. The AMF/SEAF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF as currently specified in TS 33.501 [2]. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [4].

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 as currently specified in TS 33.501 [2]. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [4].

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 to run primary authentication using EAP-TTLS. The UDM provides the AUSF also with the address of the CdP if required. CdP UE ID is also provided if available in the subscription data.

6. Based on the indication from the UDM, the AUSF runs EAP-TTLS phase 1 towards the UE as specified in RFC 5281 [5]. The AUSF starts EAP-TTLS by sending 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 EAP-Request [EAP-TTLS] message whose data field encapsulates a TLS ServerHello message, a TLS ServerCertificate message, a TLS ServerKeyExchange message, an optional CertificateRequest message, and a TLS ServerHelloDone message. Such EAP-Request message, denoted as EAP-Request [EAP-TTLS, ServerHello, ServerCertificate, ServerKeyExchange, CertificateReuest\*, ServerHelloDone], 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, CertificateReuest\*, ServerHelloDone] message in an Authentication Request message, including the ngKSI and the ABBA parameters.

12. The UE authenticates the AUSF by validating the server certificate included in the EAP-Request message received in step 11. The UE needs to be provisioned with certificates of a trust anchor to validate the AUSF 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 ClientCertificate message if a CertifiateRequest messages was received in step 11, a TLS ClientKeyExchange message, an optional CertificateVerify message, a TLS ChangeCipherSpec message, and a TLS Finished message. This EAP-Response message is denoted as EAP-Response [EAP-TTLS, ClientCertificate\*, ClientKeyExchange, CertifiateVerify\*, 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.

15a. The AUSF verifies the client certificate if received in step 14.

15b. 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, denoted as EAP-Request [EAP-TLS, ChangeCipherSpec Finished], 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 AUSF 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 towards the AAA-H as specified in RFC 5281 [5].

18. After successful authentication, an EMSK is established from the keying materials obtained in step 16. The AUSF derives the KAUSF from the EMSK as described in 33.501 [2] (using the 256 msb of the EMSK as KAUSF). The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6 of 33.501 [2].

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

20. The AMF/SEAF forwards to the UE the EAP-Success message 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 step 16. The UE further derives the KAUSF and the KSEAF according to 3GPP TS 33.501 [2].

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