**3GPP TSG-SA3 Meeting #102-e *S3-210344***

**e-meeting, 18th - 29th January 2021** Revision of S3-20xxxx

**Source: Ericsson**

**Title: Resolving EN on SUPI privacy in Solution#1**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***It is proposed to resolve one of the ENs in solution #1 of [1].***

# 2 References

 [1] 3GPP TR 33.857: "Study on enhanced security support for Non-Public Networks"

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

# 3 Rationale

 In solution #1 of TR 33.857 [1] there is an Editor's note:

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

Annex I.5 of TS 33.501 [2] states:

" The UE shall support SUPI privacy as defined in clause 6.12 with the following exception. When using an authentication method other than 5G AKA or EAP-AKA', the location of the functionality related to SUPI privacy in the UE is out of scope.

Furthermore, the privacy considerations for EAP TLS (given in Annex B.2.1.2) should be taken into account when using an authentication method other than 5G AKA or EAP-AKA'. "

Hence SUPI privacy is already specified in TS 33.501 [3] for all key-generating EAP-methods and the Editor's note can be removed.

# 4 Detailed proposal

\*\*\*\*\*\*BEGIN CHANGES\*\*\*\*\*

## 6.1 Solution #1: Primary authentication between an SNPN and third-party AAA server using EAP

### 6.1.1 Introduction

This solution address Key Issue #1 Credentials owned by an external entity, in particular the case where the separate entity is deployed as a AAA server. It is assumed that the AAA server is some existing solution. Hence, no updates to the AAA server can be made.

The assumed architecture is described in TR 23.700-7 [3], clause 6.8.2.2. An illustration is provided here for convenience in Figure 6.1.1-1. The SNPN includes a complete 5GS SNPN network and the CdP is the Credential provider (AAA server in this case).



Figure 6.1.1-1: Access to SNPN services using credentials from Credential Provider (CdP) for authentication in the SNPN

### 6.1.2 Solution Details

This solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN. The credential provider will typically correspond with an already existing credential management system owned by the vertical owner of the SNPN 5GS.

The UE is provisioned with credentials (for any key-generating EAP method) managed by the CdP, which include an identifier and related security information and the CdP Identifier. The UE initiates registration in the SNPN using a SUCI based on the network-specific identifier, provided by the CdP and provisioned in the UE.

For the primary authentication procedure, the UDM allows the UE to run primary authentication with credentials owned by a certain CdP. The UDM indicates to the AUSF to proceed with primary authentication involving the corresponding CdP.

In this scenario the authentication server role is taken by the AAA. The AUSF acts as EAP authenticator and interacts with the AAA to execute the primary authentication procedure.

The shift of the AAA being the AAA server will result in an impact on the key hierarchy. The KAUSF is in this scenario derived from MSK instead of EMSK. This leads to impact on the UE and AUSF and also in the primary authentication procedure in the sense that an indication could be sent to the UE that the alternative key hierarchy is to be applied.

#### 6.1.2.1 Procedure



Figure: 6.1.2-1: 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.

It is further assumed that there exists a trust relation between the AUSF (AAA-IWF) and the AAA. These entities need to be mutually authenticated, and the information transferred on the interface need to be confidentiality, integrity and replay protected.

1. The UE selects the SNPN and initiates UE registration in the SNPN. In case no SUPI is provisioned in the UE, the UE creates a SUCI based on the CdP-UE ID provided by the CdP and provisioned in the UE.

NOTE 1: In the case of the UE constructing the SUCI from CdP-UE ID, it is assumed that the CdP-UE ID 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].

2. The AMF 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, with an external entity based on subscription data or by looking at the realm part of the SUPI in NAI format.

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 with credentials owned by a certain CdP. 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 interacts with the CdP to execute the primary authentication procedure. The AUSF derives the CdP-UE ID from the SUPI unless received from UDM. The AUSF uses a AAA-P/IWF to interact with the CdP.

7. The UE executes the applicable authentication method with the CdP.

8. After successful authentication, the AUSF is provided by the MSK from the AAA.

9. The AUSF uses the most significant 256 bits of MSK as the KAUSF. The AUSF also derives KSEAF from the KAUSF as defined in Annex A.6 of 33.501 [2].

Editor's note: It is FFS if other input, not known to the external AAA is to be used for input when deriving the KAUSF from MSK.

10. The AUSF sends to the AMF the successful indication together with the SUPI of the UE and the resulting KSEAF, and optionally an indicator that MSK has been used.

11. The AMF sends the MSK indicator to the UE in a NAS message

12. The UE decides to derive the KAUSF from MSK instead of EMSK, either based on the indicator received from AMF or by interpretation of the realm part of the NAI that might indicate the use of external CdP.

Editor's note: It is FFS whether the UE instead of the above can be pre-configured with the information which key derivation method to use.

### 6.1.3 System impact

**UE**

KAUSF is derived from MSK instead of EMSK. The decision to do this can be based on an indicator received from the AMF or by interpretation of the realm part of the UE ID in NAI format.

**AMF**

Relay of new MSK indicator

**UDM**

Decision if external authentication is to be triggered, e.g. by interpreting the realm part of NAI or by UE subscription data.

**AUSF**

KAUSF is derived from MSK instead of EMSK.

Send new indicator towards AMF indicating MSK usage.

**AAA-S**

None

### 6.1.4 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

The solution fulfils the potential security requirements of KI#1 and shows how a key-generating EAP method can be used as primary authentication with a separate entity.

UE and AUSF are impacted by the use of a new key hierarchy option.

As a result of the proposed solution, the CdP will be able to derive the KAUSF from the MSK. As a consequence of this, the CdP could use this to compromise security mechanisms based on KAUSF. Because of this, a the CdP must be trusted by the SNPN.

To protect the transfer of the MSK, the interface between AAA-IWF and the AAA needs security measures to prevent the MSK (and thereby KAUSF) from being compromised by any external parties.

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