**3GPP TSG-SA3 Meeting #104e-Ad-hoc** ***S3-213514***

**e-meeting, 27 – 30 September 2021**

**Source: Ericsson**

**Title: Removing Editor's notes in I.2.2.z**

**Document for: Approval**

**Agenda Item: 4.5**

# 1 Decision/action requested

***Approve this contribution to be included in the eNPN living document [1].***

# 2 References

[1] S3-2132006, Security aspects of eNPN (living document)

[2] [C4-214856](https://www.3gpp.org/ftp/tsg_ct/WG4_protocollars_ex-CN4/TSGCT4_105e_meeting/Docs/C4-214856.zip), Authentication by AAA server in CH

# 3 Rationale

This document provides updates to resolve the Editor's notes in clause I.2.2.z ("Credentials holder using AAA server for primary authentication").

In the following clauses the Editor's notes are discussed and actions proposed.

## 3.1 UE Credentials

Editor's Note: How the credentials are provisioned in the UE is FFS.

**Discussion:** Since there is still no conclusion on how the UE credentials are provisioned to the UE, this E.N. remains.

## 3.2 SUPI privacy

Editor's Note: It is FFS if only SUCI using null scheme with anonymised SUPI should be supported for this use case.

**Discussion:** In the case of using EAP authentication towards an external CH using AAA, SUCI null scheme together with anonymised SUCI can be used as specified in Annex B. Meanwhile it is also possible to use SUPI privacy mechanisms as specified in clause 6.12 of 33.501 if a public key is provisioned in the UE. In this case, the UDM de-conceals the SUCI (not the AAA).

Even if no USIM is present, the public key might be available elsewhere according to Annex I, clause I.5:

" 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."

**Proposal:** With reference to the discussion above the E.N is removed.

There are some other E.N.s related to SUPI privacy:

Editor's Note: It is FFS if the SUPI needs to be sent to the external entity (AAA).

Editor's Note: If the SUPI is also included as part of the messages in step 9 and 10 is FFS.

**Discussion:** Normally SUPI is never exposed to external entities. However, the AAA holds the credentials of the UE and is the entity responsible of authenticating the UE. It is also assumed to be a trust relation between the SNPN and the AAA. There are two cases:

* In the case of anonymised SUPI, it is only after a performed authentication that the AAA learns the identity of the UE (SUPI). The SUPI needs to be returned to the AUSF together with a successful authentication result.
* Even if anonymised SUPIs are not used, the AUSF knows the SUPI that the UE provided, but it is only after the authentication by the AAA that the AUSF can be certain that it is the real SUPI of the authenticated UE. Hence, also in this case the SUPI needs to be returned from the AAA to the AUSF after a successful authentication.

**Proposal:** Sending the SUPI to the AAA in step 7 is not necessary since the AAA will learn the SUPI during the authentication. SUPI is removed as data in step 7. The SUPI is added as data in steps 9 and 10 to provide the AUSF with the SUPI of the authenticated device. Further clarifications are added for the use of anonymous SUPI/SUCI. The E.N.s above are removed with respect to the discussion above and the proposed changes.

## 3.3 UDM involvement

Editor's Note: It is FFS why the existing UDM service with mandatory IE 'Authentication method' need to be invoked for an authentication based on credentials held by an external entity.

**Discussion**: It has now been decided in CT4 [2] to add a new IE in the Nudm\_UEAU\_Get response that signals to the AUSF to use an external entity for authentication. When this new value is used the 'Authentication method' value shall be set to 'NONE'.

**Proposal:** The procedures are updated to reflect the decision in CT4. We also add the possibility that the AUSF may skip the interaction with UDM in case of anonymous SUCI and decide to execute primary authentication based on local configuration or realm part of SUPI. By that the E.N. should no longer be needed and is thus removed.

## 3.4 AUSF-NSSAAF-AAA interfaces

Editor's Note: The details of the interface and protocol between AUSF and AAA are FFS.

**Discussion**: The interface between AUSF and NSSAAF is new and a new service operation (Nnssaaf\_AIW\_Authenticate) was added to the living document during the last meeting. This interface should need no further definition.

The interface between NSSAAF and AAA already exists and is used for slice and secondary authentication. In step 7 of the procedure the message was erroneously named as EAP message. This is now aligned with the procedures for slice specific authentication in clause 16.3 of 33.501using the term "AAA protocol". This term is also used step in 9.

**Proposal:** With reference to the discussion above the E.N is removed.

## 3.5 Alignment with 23.501

Editor's note: It is FFS if and how clause 1.2.2.3 aligns with TS 23.501 5.30.2.9.2 Credentials Holder using AAA Server for primary authentication and authorization

**Discussion:** It is not clear if and how the procedures described in I.2.2.z misalign with 23.501, clause 5.30.2.9.2.

**Proposal**: It is proposed to remove this Editor's note and, if needed, replace it with one that specifies in detail what needs to be aligned.

## 3.6 MSK indication

Editor's note: It is FFS how the UE will be configured to know to use MSK instead of EMSK.

**Discussion:** Since there is still no conclusion on how the indication to the UE can be made, this E.N. remains.

## 3.7 EAP-methods

**Proposal**: On more change is proposed that is not related to any Editor's note. It is proposed to clarify that the procedures for "Credentials holder using AAA server for primary authentication" are to be used for key generating EAP-methods other than EAP-AKA' (and EAP-AKA). The reason is that in case an external entity support EAP-AKA', the 5GS roaming architecture is reused as concluded in KI#1 of the TR.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGES \*\*\*

### I.2.2.z Credentials holder using AAA server for primary authentication

#### I.2.2.z.1 General

The procedures described in this clause enables UEs to access an SNPN which makes use of a credential management system managed by a credential holder external to the SNPN.

In this scenario the authentication server role is taken by the AAA Server. The AUSF acts as EAP authenticator and interacts with the AAA Server to execute the primary authentication procedure, where the AAA server supports some key generating EAP-method other than EAP-AKA or EAP-AKA'.

The architecture for SNPN access using credentials from a Credentials Holder using AAA Server is described in clause 5.30.2.9.2 of TS 23.501 [2].

I.2.2.z.2 Procedure

****

**Figure: I.2.2.z.2-1: Primary authentication with external domain**

0. The UE shall be configured with credentials from the Credentials holder e.g. SUPI containing a network-specific identifier and credentials for any key-generating EAP-method.

Editor's Note: How the credentials are provisioned in the UE is FFS.

It is further assumed that there exists a trust relation between the SNPN and the Credentials holder AAA Server. 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 shall select the SNPN and initiate UE registration in the SNPN.

For construction of the SUCI, existing methods in clause 6.12 can be used. If the home network public key of the SNPN is not provisioned in the UE, the UE shall create a SUCI using null scheme with anonymised SUPI as described in Annex B.

2. The AMF within the SNPN shall initiate a primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF. The AMF shall select an AUSF based on the HNI of the SUCI (*i.e. realm for NSI SUPI type*) presented by the UE as specified in TS 23.501 [2].

3. The AUSF shall initiate a Nudm\_UEAuthentication\_Get service operation. The AUSF shall select a UDM also using the SUCI/SUPI provided by the AMF as specified in TS 23.501 [2].

NOTE 1: SUPI will be used instead of SUCI in the case of a re-authentication.

4. In case the UDM receives a SUCI, the UDM shall resolve the SUCI to the SUPI before checking the authentication method applicable for the SUPI. The UDM decides to run primary authentication with an external entity based on subscription data or by looking at the realm part of the SUPI in NAI format.

When anonymous SUCI is used, the UDM can still decide based on the realm part of SUPI, perhaps in combination with subscription data that primary authentication is to be run with an external entity. Alternatively, the AUSF may skip the interaction with UDM and decide to execute primary authentication based on local configuration or realm part of SUPI.

5. The UDM shall provide the AUSF with the UE SUPI and shall indicate to the AUSF to run primary authentication with an external Credentials holder.

When anonymous SUCI is used, the UDM returns an anonymous SUPI to the AUSF.

6. Based on the indication from the UDM, the AUSF shall select an NSSAAF as defined in 3GPP TS 23.501 [2] and initiate a Nnssaaf\_AIWF\_Authenticate service operation towards that NSSAAF as defined in section 14.4.x.

7. The NSSAAF shall select AAA Server based on the domain name corresponding to the realm part of the SUPI provided by the UDM to the AUSF in step 5 (e.g. SUPI or anonymous SUPI). The NSSAAF shall perform related protocol conversion and relay messages to the AAA Server.

8. The UE and AAA Server shall perform mutual authentication. The AAA Server shall act as the EAP Server for the purpose of primary authentication.

When anonymous SUCI/SUPI, the AAA-Server determines the SUPI of the UE using EAP authentication method dependent procedures and is outside the scope of this specification. 9. After successful authentication, the MSK and the SUPI shall be provided from the AAA Server to the NSSAAF.

10. The NSSAAF returns the MSK and the SUPI to the AUSF using the Nnssaaf\_AIWF\_Authenticate service operation response message.

11. Before deriving any keys, the AUSF verifies that the SUPI received from UDM in step 5 matches the SUPI received from NSSAAF. The AUSF shall use the most significant 256 bits of MSK as the KAUSF. The AUSF shall also derive KSEAF from the KAUSF as defined in Annex A.6.

12. The AUSF shall send the successful indication together with the SUPI of the UE to the AMF together with the resulting KSEAF.

13. The AMF shall send the EAP success in a NAS message.

14. The UE shall derive the KAUSF from MSK as described in step 11.

Editor's note: It is FFS how the UE will be configured to know to use MSK instead of EMSK.

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