**3GPP TSG-SA3 Meeting #104e** ***S3-212734***

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

**Source: Ericsson**

**Title: Change request to living document: EAP flow**

**Document for: Approval**

**Agenda Item: 4.17**

# 1 Decision/action requested

***Approve this contribution to be included in the draft CR for TS 33.501specifying the eNPN skeleton.***

# 2 References

[1] -

# 3 Rationale

This document provides the procedures for Credentials holder using AAA server for primary authentication and additional requirements on the NSSAAF resulting from the new procedures. The procedure flow in clause I.2.2.3 is adapted from Solution #1 in TR 33.857 with the adaptation being using normative language and aligning with SA2 decisions on architecture. (SA2 TS 23.501 and TS 23.502 specify the support of the NSSAAF to relay EAP messages towards a AAA-S or AAA-P and perform related protocol conversion as needed during primary authentication procedure between an AUSF in an SNPN and a Credentials Holder using AAA server.)

# 4 Detailed proposal

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

## 5.13 Requirements on NSSAAF

The Network slice specific and SNPN authentication and authorization function (NSSAAF) shall handle the Network Slice Specific Authentication requests from the serving AMF as specified in clause 16.The NSSAAF shall also support functionality for access to SNPN using credentials from Credentials Holder using AAA-S as specified in clause I.2.2.3.

The NSSAAF is responsible to send the NSSAA requests to the appropriate AAA-S.

The NSSAAF shall support AAA-S triggered Network Slice-Specific Re-authentication and Re-authorization and Slice-Specific Authorization Revocation and translate any AAA protocol into a Service Based format.

NSSAAF shall translate the Service based messages from the serving AMF or AUSF to AAA protocols towards AAA-P/AAA-S.\*\*\* NEXT CHANGE \*\*\*

### 14.2.2 Nudm\_UEAuthentication\_Get service operation

**Service operation name:** Nudm\_UEAuthentication\_Get

**Description:** Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

**Inputs, Required:** SUPI or SUCI, serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS).

**Outputs, Required:** Authentication method and corresponding authentication data for a certain UE as identified by SUPI or SUCI input.

Editor's note: How the UDM indicates to the AUSF to run primary authentication with an external Credentials holder is FFS.

**Outputs, Optional:** SUPI if SUCI was used as input. AKMA Indication, if the subscriber has an AKMA subscription (see TS 33.535 [91]).

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

14.4 Services provided by NSSAAF

14.4.1 Nnssaaf\_NSSAA services

14.4.1.1 General

The following table illustrates the security related services for Network Slice Specific Authentication and Authorisation that NSSAAF provides.

**Table 14.4.1.1-1: NF services for the NSSAA service provided by NSSAAF**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name** | **Service Operations** | **Operation Semantics** | **Example Consumer(s)** |
| Nnssaaf\_NSSAA | Authenticate | Request/Response | AMF |
| Re-AuthenticationNotification | Notify | AMF |
| RevocationNotification | Notify | AMF |

14.4.1.2 Nnssaaf\_NSSAA\_Authenticate service operation

**Service operation name:** Nnssaaf\_NSSAA\_Authenticate

**Description:** NF consumer requires the NSSAAF to relay Network Slice specific authentication messages towards the corresponding AAA-S handling the Network Slice specific authentication for the requested S-NSSAI (see section 16).

**Input, Required:**

1) In the initial NSSAA requests: EAP ID Response, GPSI, S-NSSAI

2) In subsequent NSSAA requests: EAP message, GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** EAP message, GPSI, S-NSSAI

**Output, Optional:** None

14.4.1.3 Nnssaaf\_NSSAA\_Re-AuthenticationNotification service operation

**Service operation name:** Nnssaaf\_NSSAA\_Re-AuthenticationNotification

**Description:** NSSAAFnotifies the NF consumer to trigger a Network Slice specific reauthentication procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nnssaaf\_NSSAA\_Re-authenticationNotification service operation.

**Input, Required:** GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

14.4.1.4 Nnssaaf\_NSSAA\_RevocationNotification service operation

**Service operation name:** Nnssaaf\_NSSAA\_RevocationNotification

**Description:** NSSAAFnotifies the NF consumer to trigger a Network Slice specific revocation procedure for a given UE and S-NSSAI.

NOTE: The AMF is implicitly subscribed to receive Nnssaaf\_NSSAA\_RevocationNotification service operation.

**Input, Required:** GPSI, S-NSSAI

**Input, Optional:** None

**Output, Required:** None

**Output, Optional:** None

14.4.X Nnssaaf\_AIW services

14.4.X.1 General

The following table illustrates the security related services provided by the NSSAAF for primary authentication in SNPN with Credentials holder using AAA server (see section I.2.2.3).

**Table 14.4.X.1-1: NF services for CH using AAA for primary authentication provided by NSSAAF**

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Example Consumer(s) |
| Nnssaaf\_AIW | Authenticate | Request/Response | AUSF |

14.4.X.2 Nnssaaf\_AIW\_Authenticate service operation

**Service operation name:** Nnssaaf\_AIW\_Authenticate

**Description:** The NSSAAF provides Authentication and Authorization service to the consumer NF by relaying EAP messages towards a AAA-S or AAA-P and performing related protocol conversion as needed. **Input, Required:**

1) In the initial authentication request: SUPI.

2) In subsequent authentication requests: EAP message.

**Input, Optional:** None

**Output, Required:** EAP message, authentication result and if success MSK.

**Output, Optional:** None

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

### I.2.2.3 Credentials holder using AAA server for primary authentication

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

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

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

#### I.2.2.3.1 Procedure



Figure: I.2.2.3.1-1: 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-S. 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.

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

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: 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.NOTE: 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 shall be run with an external entity.

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.

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. The NSSAAF shall perform related protocol conversion and relay EAP messages to the AAA Server (or AAA proxy).

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

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

9. After successful authentication, the MSK shall be provided from the AAA-S to the NSSAAF.

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

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

11. 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.

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

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