**3GPP TSG-SA3 Meeting #104-e *draft\_S3-213206-r1***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **draft-CR** | **rev** | **<Rev#>** | **Current version:** | **<Version#>** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Security aspects of eNPN | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2021-09-03 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Security aspects for the Enhanced support of Non-Public Networks need to be specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Enhancements to 5GS on the security aspects for the Enhanced support of Non-Public Networks. Specifically:  - Impact on primary authentication and key hierarchy when the credentials are owned by an external entity:  - Credentials holder using AUSF and UDM for primary authentication  - Credentials holder using AAA server for primary authentication  - Impact on roaming-related security mechanisms.  Change history of the living document:  SA3#104-e:   * S3-213235 (Service authorization in SNPNs with Credentials Holder using AUSF and UDM for primary authentication as external entity) * S3-213203 (EAP flow) * S3-213201 (Key hierarchy) * S3-213205 (Credentials holder using AUSF and UDM for primary authentication) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Enhanced support of Non-Public Network will not have necessary security aspects specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.9.3.2, 5.13, 13.4.1.2.2, 14.2.2, 14.4.1.1, 14.4.1.2, 14.4.1.3, 14.4.1.4, 14.4.X (new), 14.4.X.1 (new), 14.4.X.2 (new), Annex I.2.2.x (new), Annex I.2.2.z (new), Annex I.2.2.z.1 (new), Annex I.2.2.z.2 (new), Annex I.2.3.x (new), Annex I.2.3.y (new), Annex I.2.a,(new), Annex I.x (new), Annex I.x.1 (new), Annex I.a (new), Annex I.a.1 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

Annex I (normative):  
Non-public networks

I.1 General

This Annex provides details on security for non-public networks. Most of the security procedures are the same as public networks so this annex only summarizes and specifies where there are exceptions to the normal procedures.

The feature for support of non-public networks (NPN) by 5GS is described in clause 5.30 of 23.501 [2].

Editor's Note: Security aspects for other NPN issues including PNiNPN are ffs.

I.2 Authentication in standalone non-public networks

I.2.1 General

One of the major differences of non-public networks is that authentication methods other than AKA based ones may be used in a standalone non-public network (SNPN). When an AKA-based authentication method is used, clause 6.1 shall apply. When an authentication method other than 5G AKA or EAP-AKA' is used, only the non-AKA specific parts of clause 6.1 shall apply. An example of running such an authentication method is given in Annex B with EAP-TLS.

The choice of the supported authentication methods for access to SNPNs follows the principles described in clauses I.2.2 and I.2.3.

I.2.2 EAP framework, selection of authentication method, and EAP method credentials

### I.2.2.x General

The EAP authentication framework is supported by the 5GS as described in clause 6.1.1.2.

The UE and the serving network may support 5G AKA, EAP-AKA', or any other key-generating EAP authentication method.

Selection of the authentication methods is dependent on NPN configuration.

NOTE 1: For EAP-AKA' (as well as 5G AKA), the selection is described in clause 6.1.2. For authentication, that is not using EAP-AKA' (or 5G AKA), the selection is NPN operator deployment specific and out of scope of this specification.

When an EAP authentication method other than EAP-AKA' is selected, the chosen method determines the credentials needed in the UE and network. These credentials, called the EAP-method credentials, shall be used for authentication.

NOTE 2: How credentials for EAP methods other than EAP-AKA' are stored and processed within the UE is out of the scope for standalone non-public networks.

NOTE 3: Storage and processing of credentials for EAP-AKA' (as well as 5G AKA) is described in clause 6 of the present document.

### 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 provider 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.

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.

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.

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.

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 is to 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.

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

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

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.

9. After successful authentication, the MSK shall be provided from the AAA Server 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.

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

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

I.2.3 Key hierarchy, key derivation and key distribution

### I.2.3.x General

The text in clauses 6.2.1 and 6.2.2 cannot apply directly for an EAP authentication method other than EAP-AKA' as these clauses assume that an AKA-based authentication method is used. The major differences are the way in which KAUSF is calculated and that the UDM/ARPF is not necessarily involved in the key derivation or distribution.

Depending on the selected authentication method, the KAUSF is generated as follows:

- For 5G AKA and EAP-AKA' refer to clause 6.2.1.

- When using a key-generating EAP authentication method other than EAP-AKA', the key derivation of KAUSF is based on the EAP-method credentials in the UE and AUSF and shall be done as shown in Figure I.2.3-1.

NOTE: For EAP authentication methods other than EAP-AKA', this key derivation replaces clauses 6.2.1 and 6.2.2 for the generation of KAUSF .



**Figure I.2.3-1: KAUSF derivation for key-generating EAP authentication methods other than EAP-AKA'**

KAUSF shall be derived by the AUSF and UE from the EMSK created by the EAP authentication as for EAP-AKA'.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the KAUSF downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from KAUSF (e.g. KSEAF, KAMF, KgNB etc) apply without modification.

### I.2.3.y Credentials holder using AAA server for primary authentication

When running primary authentication towards an external Credentials holder using AAA server for authentication as specified in clause I.2.2.z the derivation of KAUSF is based on the EAP-method credentials in the UE and AAA-S and shall be done as shown in Figure I.2.3.y-1.

EAP method credentials

EAP

authentication

MSK

K

AUSF

**Figure I.2.3.y-1: KAUSF derivation for primary authentication towards an external Credentials holder using AAA server**

KAUSF shall be derived by the AUSF and UE from the MSK derived during the EAP authentication as specified in clause I.2.2.z.1.

All of figures 6.2.1-1, 6.2.2.1-1 and 6.2.2.2.2-1 from the KAUSF downwards are used without modification. Similarly, text relating to the key hierarchy, key derivation and key distribution in clauses 6.2.1, 6.2.2.1 and 6.2.2.2 for keys derived from KAUSF (e.g. KSEAF, KAMF, KgNB etc) apply without modification.

### I.2.a Credentials Holder using AUSF and UDM for primary authentication

I.3 Serving network name for standalone non-public networks

I.3.1 General

The identification of standalone non-public networks uses Network Identifier (NID) in addition to PLMN ID. This means the definition of SN Id in clause 6.1.1.4.1 for the derivation of KSEAF for all authentication methods, CK' and IK' for EAP-AKA', and KAUSF and (X)RES\* for 5G AKA needs modification for standalone non-public networks.

I.3.2 Definition of SN Id for standalone non-public networks

For standalone non-public networks, the SN Id (used in the input for various key/parameter derivations) identifies the serving SNPN.

It is defined as follows:

SN Id = PLMN ID:NID

and is specified in detail in TS 24.501 [35].

I.4 Modification of CAG ID list in the UE

The following requirements apply to NAS messages that modify the list of CAG IDs stored in the UE:

- the AMF shall only send such a NAS message once NAS security has been established; and

- the UE shall only modify its list of CAG IDs after successful integrity verification of the integrity protected NAS message requesting such a modification.

I.5 SUPI privacy for standalone non-public networks

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'.

I.6 Authentication in Public Network Integrated Non-Public Networks (PNI-NPN)

For public network integrated NPN (PNI-NPN), the primary authentication shall be performed with the public network as described in clause 6.1. Secondary authentication as described in clause 11 and slice-specific authentication as described in the main body can take place after a successful primary authentication.

# I.x Authorization aspects in SNPNs

## I.x.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, service authorization as specified in clause 13.4.1.2 applies.

I.a SEPP and interconnect related security procedures

I.a.1 Credentials holder using AUSF and UDM for primary authentication

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, clause 5.30.2.9.3 of TS 23.501 [2] states that the UE is not considered to be roaming, however SNPN and Credentials Holder communicate via SEPPs.

The following requirements and procedures related to SEPPs and interconnect security apply for SNPNs with Credentials Holder using AUSF and UDM for primary authentication:

- Requirements for Security Edge Protection Proxy (SEPP), clause 5.9.3.2

- Protection between SEPPs, clause 13.1.2.

NOTE: IPX providers are not expected to be used between SNPN and Credentials holder using AUSF and UDM for primary authentication.

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

5.9.3.2 Requirements for Security Edge Protection Proxy (SEPP)

The SEPP shall act as a non-transparent proxy node.

The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other.

The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network.

The SEPP shall handle key management aspects that involve setting up the required cryptographic keys needed for securing messages on the N32 interface between two SEPPs.

The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties.

As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs.

The receiving SEPP shall be able to verify whether the sending SEPP is authorized to use the PLMN ID or SNPN ID in the received N32 message.

The SEPP shall be able to clearly differentiate between certificates used for authentication of peer SEPPs and certificates used for authentication of intermediates performing message modifications.

NOTE 1: Such a differentiation could be done e.g. by implementing separate certificate storages.

The SEPP shall discard malformed N32 signaling messages.

The sending SEPP shall reject messages received from the NF (directly or via SCP) with JSON including "encBlockIndex" (regardless of the encoding used for that JSON request).

The receiving SEPP shall reject any message in which an IPX has inserted or relocated references to encBlockIndex.

The SEPP shall implement rate-limiting functionalities to defend itself and subsequent NFs against excessive CP signaling. This includes SEPP-to-SEPP signaling messages.

The SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).

NOTE 2: An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP’s own PLMN, the message is discarded.

The SEPP shall be able to use one or more PLMN IDs. In the situation that a PLMN is using more than one PLMN ID, this PLMN's SEPP may use the same N32-connection for all of the PLMN's PLMN IDs, with each of the PLMN's remote PLMN partners. If different PLMNs are represented by the PLMN IDs supported by a SEPP, the SEPP shall use separate N32-connections for each pair of home and visited PLMN.

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

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 Server as specified in clause I.2.2.z.

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 \*\*\*

13.4.1.2 Service access authorization in roaming scenarios

13.4.1.2.1 OAuth 2.0 roles

In the roaming scenario, OAuth 2.0 roles are as follows:

a. The visiting Network Repository Function (vNRF) shall be the OAuth 2.0 Authorization server for vPLMN and authenticates the NF Service Consumer.

b. The home Network Repository Function (hNRF) shall be OAuth 2.0 Authorization server for hPLMN and generates the access token.

c. The NF Service Consumer in the visiting PLMN shall be the OAuth 2.0 client.

d. The NF Service Producer in the home PLMN shall be the OAuth 2.0 resource server.

**OAuth 2.0 client (NF Service Consumer) registration with the OAuth 2.0 authorization server (NRF) in the vPLMN**

Same as in the non-roaming scenario in 13.4.1.1.

**OAuth 2.0 resource server (NF Service Producer) registration with the OAuth 2.0 authorization server (NRF) in the hPLMN**

Same as in the non-roaming scenario in 13.4.1.1.

13.4.1.2.2 Service Request Process

The complete service request is two-step process including requesting an access token by NF Service Consumer (Step 1, i.e. 1a or 1b), and then verification of the access token by NF Service Consumer (Step 2).

**Step 1: Access token request**

Pre-requisite:

- The NF Service consumer (OAuth2.0 client) is registered with the vNRF (Authorization Server in the vPLMN).

- The hNRF and NF service producer share the required credentials. Additionally, the NF Service producer (OAuth2.0 resource server) is registered with the hNRF (Authorization Server in the hPLMN) with "additional scope" information per NF type.

- The two NRFs have mutually authenticated each other.

- The NRF in the serving PLMN and NF service consumer have mutually authenticated each other.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Consumer and the vNRF are located in the SNPN while the hNRF is located in the Credentials Holder.

**1a. Access token request for accessing services of NF Service Producers of a specific NF type**

The following procedure describes how the NF Service Consumer obtains an access token for NF Service Producers of a specific NF type for use in the roaming scenario.

****

**Figure 13.4.1.2.2-1: NF Service Consumer obtaining access token before NF Service access (roaming)**

1. The NF Service Consumer shall invoke Nnrf\_AccessToken\_Get Request (NF Instance Id of the NF Service Consumer, the requested "scope" including the expected NF Service Name (s) and optionally "additional scope" information (i.e. requested resources and requested actions (service operations) on the resources), NF Type of the expected NF Service Producer instance, NF type of the NF Service Consumer, home and serving PLMN IDs, optionally list of NSSAIs or list of NSI IDs for the expected NF Service Producer instances, optionally NF Set ID of the expected NF Service Producer) from NRF in the same PLMN.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the V-SNPN ID is included instead of the serving PLMN ID and the <?> is included instead of the home PLMN ID.

Editor's Note: The ID of the Credentials Holder to be included instead of the home PLMN ID needs to be clarified.

2. The NRF in serving PLMN shall identify the NRF in home PLMN (hNRF) based on the home PLMN ID, and request an access token from hNRF as described in clause 4.17.5 of TS 23.502 [8]. The vNRF shall forward the parameters it obtained from the NF Service Consumer, including NF Service Consumer type, to the hNRF.

3. The hNRF checks whether the NF Service Consumer is authorized to access the requested service(s). If the NF Service Consumer is authorized, the hNRF shall generate an access token with appropriate claims included as defined in clause 13.4.1.1. The hNRF shall digitally sign the generated access token based on a shared secret or private key as described in RFC 7515 [45]. If the NF service consumer is not authorized, the hNRF shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer appended with its PLMN ID (subject), NF type of the NF Service Producer appended with its PLMN ID (audience), expected services name(s), (scope) and expiration time (expiration), and optionally "additional scope" information (allowed resources and allowed actions (service operations) on the resources). The claims may include a list of NSSAIs or NSI IDs for the expected NF Service Producer instances. The claims may include the NF Set ID of the expected NF Service Producer instances.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the V-SNPN ID is included instead of the NF Service Consumer's PLMN ID and the <?> is included instead of the NF Service Producer's PLMN ID.

Editor's Note: The ID of the Credentials Holder to be included instead of the Producer's PLMN ID needs to be clarified.

4. If the authorization is successful, the access token shall be included in Nnrf\_AccessToken\_Get Response message to the vNRF. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43].

5. The vNRF shall forward the Nnrf\_AccessToken\_Get Response or error message to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Service Producer NF type listed in claims (scope, audience) during their validity time. The other parameters (e.g., the expiration time, allowed scope) sent by NRF in addition to the access token are described in TS 29.510 [68].

**1b. Obtain access token for accessing services of a specific NF Service Producer instance / NF Service Producer service instance**

The following steps describes how the NF Service Consumer obtains an access token before service access to a specific NF Service Producer instance / NF Service Producer service instance.

1. The NF Service Consumer shall request an access token from the NRF for a specific NF Service Producer instance / NF Service Producer service instance. The request shall include the NF Instance Id of the requested NF Service Producer, appended with its PLMN ID, the expected NF service name and NF Instance Id of the NF Service Consumer, appended with its PLMN ID.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the V-SNPN ID is included instead of the NF Service Consumer's PLMN ID and the <?> is included instead of the NF Service Producer's PLMN ID.

Editor's Note: The ID of the Credentials Holder to be included instead of the Producer's PLMN ID needs to be clarified.

2. The NRF in the visiting PLMN shall forward the request to the NRF in the home PLMN.

3. The NRF in the home PLMN checks whether the NF Service Consumer is authorized to use the requested NF Service Producer instance/NF Service Producer service instance and shall then proceed to generate an access token with the appropriate claims included. If the NF Service Consumer is not authorized, the NRF in the home PLMN shall not issue an access token to the NF Service Consumer.

The claims in the token shall include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service Consumer appended with its PLMN ID (subject), NF Instance Id of the requested NF Service Producer appended with its PLMN ID (audience), expected service name(s) (scope) and expiration time (expiration).

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the V-SNPN ID is included instead of the NF Service Consumer's PLMN ID and the <?> is included instead of the NF Service Producer's PLMN ID.

Editor's Note: The ID of the Credentials Holder to be included instead of the Producer's PLMN ID needs to be clarified.

4. The token shall be included in the Nnrf\_AccessToken\_Get response sent to the NRF in the visiting PLMN.

5. The NRF in the visiting PLMN shall forward the Nnrf\_AccessToken\_Get response message to the NF Service Consumer. The NF Service Consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from NF Instance Id or several NF Instance Id(s) of the requested NF Service Producer listed in claims (scope, audience) during their validity time.

**Step 2:Service access request based on token verification**

In addition to the steps described in the non-roaming scenario in 13.4.1.1, the NF Service Producer shall verify that the PLMN-ID contained in the API request is equal to the one inside the access token.

****

**Figure 13.4.1.2.2-2: NF Service Consumer requesting service access with an access token in roaming case**

The NF Service Producer shall check that the home PLMN ID of audience claim in the access token matches its own PLMN identity.

For SNPNs with Credentials Holder using AUSF and UDM for primary authentication, the NF Service Producer verifies the V-SNPN ID contained in the API request instead of the PLMN-ID, and the <?> instead of the home PLMN ID.

Editor's Note: The ID of the Credentials Holder to be verified instead of the home PLMN ID needs to be clarified.

The pSEPP shall check that the serving PLMN ID of subject claim in the access token matches the remote PLMN ID corresponding to the N32-f context Id in the N32 message.

\*\*\* 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.z).

**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 Server 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

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