**3GPP TSG-SA3 Meeting #105-e *draft\_S3-214437-r1***

e-meeting, 8 - 19 November 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** | **0** |  |
|  | | | | | | | | |
| *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:*** | Living document for eNPN: draftCR to TS 33.501 capturing Security aspects of eNPN | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Huawei, HiSilicon, Qualcomm Incorporated, CableLabs, Charter Communications, Intel, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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)   SA3#104-e ad-hoc   * S3-213380 (Add EN for AUSF selection in SNPN) * S3-213595 (Annex on EAP-TTLS) * S3-213661 (EN removal of Credential Holder's ID) * S3-213578 (Credentials Holder using AUSF and UDM for primary authentication)   SA3#105-e   * S3-214483 (Clarification on anonymous SUCI related) * S3-214515 (Resolution of editor note related to selection of root key) * S3-214439 (Resolution for EN on sending SUPI to SNPN) * S3-214484 (Update Nnssaaf\_AIW interface) * S3-214543 (Securing initial access for UE onboarding) | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Enhanced support of Non-Public Network will not have necessary security aspects specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3, 3.1, 3.2, 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), Annex.I.Y (new), Annex I.Y.1 (new), Annex I.Y.2 (new), Annex I.Y.2.1 (new), Annex I.Y.2.2 (new), Annex I.Y.2.3 (new), Annex I.Y.2.4 (new), Annex X (new), Annex X.1 (new), Annex X.2 (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 the key-generating EAP-method used. As part of configuration of the credentials, the UE shall also be configured with an indication that the UE shall use MSK for the derivation of KAUSF after the success of the primary authentication. The exact procedures used to configure the UE are not specified in this document.

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].

Editor’s Note: It is FFS how does the AMF selects AUSF in step 2 using realm part of SUPI which is also used for NSSAAF to select AAA server in step 7, since the AUSF and AAA server is located in different domain.

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.

In case the UDM receives an anonymous SUCI that does not contain the realm part, the UDM shall abort the procedure. If contains, the UDM authorizes the UE based on realm part of SUCI and send the anonymous SUPI and the indicator to the AUSF as described in step5.

The anonymous SUPI shall be a NAI format as described in clause B.2.1.2.2.

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.

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

When a Credentials Holder using AAA Server is used for primary authentication, the AUSF uses the MSK to derive KAUSF. It is strongly recommended that the same credentials that are used for authentication between UE and the 5G SNPN are not used for the authentication between the UE and a non-5G network, assuming that 5G SNPN and non-5G network are in different security domains.

NOTE x: MSKs obtained from the non-5G network could be used to impersonate the 5G SNPN towards the UE.

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. The EAP Identity received by the AAA Server in the EAP-Response/Identity message in step 7 may contain anonymised SUPI. In such cases, AAA Server uses the EAP-method specific EAP Identity request/response messages to obtain the UE identifier as part of the EAP authentication between the UE and the AAA Server.

9. After successful authentication, the MSK and the SUPI (i.e., the UE identifier that is used for the successful EAP authentication) 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. The SUPI received from the AAA shall be used when deriving 5G keys (e.g., KAMF) that requires SUPI as an input for the key derivation.

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 according to the pre-configured indication as described in step 0.

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

The 5G System architecture for SNPN with Credentials Holder using AUSF and UDM for primary authentication and authorization is described in clause 5.30.2.9.3 of TS 23.501 [2].

Editor's Note: Should there be any authentication related differences to TS 33.501 for the case that the CH uses AUSF and UDM for primary authentication, they can be captured in this clause.

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.

I.Y Securing initial access for UE onboarding in SNPNs

### I.Y.1 General

Onboarding of UEs for SNPNs is specified in clause 5.30.2.10 of TS 23.501 [2].

Onboarding of UEs for SNPNs allows the UE to access an Onboarding Network (ONN) based on Default UE credentials for the purpose of provisioning the UE with SNPN credentials and any other necessary information. The Default UE credentials are pre-configured on the UE.

To provision SNPN credentials in a UE that is configured with Default UE credentials, the UE selects an SNPN as ONN and establishes a secure connection (or initial access) with that SNPN referred to as Onboarding SNPN (ON-SNPN).

The present clause specifies securing of the initial access for UE onboarding.

### I.Y.2 Authentication

#### I.Y.2.1 Requirements

The primary authentication shall be performed before initial access for UE onboarding is allowed. The UE shall use Default UE credentials for the primary authentication. Credentials or means used to authenticate the UE based on Default UE credentials may be stored within the ON-SNPN or in a Default Credentials Server (DCS) that is external to the ON-SNPN.

Editor’s Note: additional requirements are FFS.

Editor’s Note: It is FFS how using anonymous SUCI or skipping default credentials identifier to initiate onboarding will meet the scope of ‘UE being verified as "uniquely identifiable and verifiably secure".

Editor’s Note: It is FFS, how the default credential identifier i.e., verifiably secure identifier is used as SUPI during the authentication procedure related to Onboarding.

#### I.Y.2.2 Primary authentication without using DCS

When the primary authentication is performed between the UE and the ON-SNPN, any one of the existing authentication methods defined in the present document may be used, i.e., 5G AKA, EAP-AKA’ or any other key-generating EAP authentication method (e.g., EAP-TLS).

The choice of primary authentication method used is left to the decision of the ON-SNPN.

#### I.Y.2.3 Primary authentication using DCS

When the primary authentication is performed between the UE and the DCS, the authentication requirements and procedures defined in clause I.2 for Credential Holder shall apply with the DCS taking the role of the Credentials Holder. When the DCS uses AAA Server for primary authentication, AUSF directly selects the NSSAAF as specified in 23.501 [2]. In this case, the UDM is not involved in the procedure defined in clause I.2.2.z.2, and the step 3 to step 5 shall be skipped.

The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.

When the primary authentication is performed between the UE and the DCS via the AUSF using EAP-TTLS, Annex X can be used.

#### I.Y.2.4 Secondary authentication using DCS

When the DCS is not involved during primary authentication, after successful primary authentication as described in I.Y.2.2, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials as described in clause 11.1.

The UE shall use Default UE credentials for the primary authentication. The secondary authentication is performed between the UE and the DCS. The secondary authentication may use the same Default UE credentials or a different UE credentials.

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

[3] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[4] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[5] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[6] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[7] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[8] 3GPP TS 23.502: "Procedures for the 5G System".

[9] 3GPP TS 33.102: "3G security; Security architecture".

[10] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[11] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[12] IETF RFC 5448: " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[13] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[14] 3GPP TS 35.215: " Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications".

[15] NIST: "Advanced Encryption Standard (AES) (FIPS PUB 197)".

[16] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation".

[17] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

[18] 3GPP TS 35.221: " Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 1: EEA3 and EIA3 specifications".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TS 22.101: "Service aspects; Service principles".

[21] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[22] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol specification".

[23] 3GPP TS 38.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[24] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[25] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)"

[26] Void

[27] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[28] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[29] SECG SEC 1: Recommended Elliptic Curve Cryptography, Version 2.0, 2009. Available <http://www.secg.org/sec1-v2.pdf>

[30] SECG SEC 2: Recommended Elliptic Curve Domain Parameters, Version 2.0, 2010. Available at <http://www.secg.org/sec2-v2.pdf>

[31] 3GPP TS 38.470: "NG-RAN; F1 General aspects and principles".

[32] 3GPP TS 38.472: "NG-RAN; F1 signalling transport".

[33] 3GPP TS 38.474: "NG-RAN; F1 data transport".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)"

[35] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[36] 3GPP TS 35.217: "Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data".

[37] 3GPP TS 35.223: "Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3; Document 3: Implementors' test data".

[38] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[39] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[40] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[41] 3GPP TS 38.460: "NG-RAN; E1 general aspects and principles".

[42] Void.

[43] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[44] IETF RFC 7519: "JSON Web Token (JWT)".

[45] IETF RFC 7515: "JSON Web Signature (JWS)".

[46] IETF RFC 7748: "Elliptic Curves for Security".

[47] IETF RFC 7540: " Hypertext Transfer Protocol Version 2 (HTTP/2)".

[48] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[49] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[50] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[53] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[54] 3GPP TS28.533: " Management and orchestration; Architecture framework".

[55] 3GPP TS28.531: "Management and orchestration of networks and network slicing; Provisioning".

[56] Void

[57] IETF RFC 7542: "The Network Access Identifier".

[58] IETF RFC 6083: " Datagram Transport Layer Security (DTLS) for Stream Control Transmission Protocol (SCTP)".

[59] IETF RFC 7516: "JSON Web Encryption (JWE)".

[60] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[61] IETF RFC 5705,"Keying Material Exporters for Transport Layer Security (TLS)".

[62] IETF RFC 5869 "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)".

[63] NIST Special Publication 800-38D: "Recommendation for Block Cipher Modes of Operation: Galois Counter Mode (GCM) and GMAC".

[64] IETF RFC 6902: "JavaScript Object Notation (JSON) Patch".

[65] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[66] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[67] Internet draft draft-ietf-emu-rfc5448bis: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[68] 3GPP TS 29.510: "5G System; Network function repository services".

[69] 3GPP TS 36.331: "Radio Resource Control (RRC); Protocol specification".

[70] 3GPP TS 29.505: "5G System; Usage of the Unified Data Repository services for Subscription Data; Stage 3".

[71] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[72] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC)".

[73] 3GPP TS 29.573: " Public Land Mobile Network (PLMN) Interconnection; Stage 3".

[74] 3GP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[75] IEEE TSN network aspects: see 3GPP TS 23.501 [2] references [95], [96], [97], [98], [104], and [107].

[76] Internet draft draft-ietf-emu-eap-tls13: "Using EAP-TLS with TLS 1.3"

[77] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[78] 3GPP TS 38.401: "NG-RAN; Architecture description".

[79] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)"

[80] IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[81] IETF RFC 2410 "The NULL Encryption Algorithm and Its Use With IPsec".

[82] Void

[83] RFC 7858: "Specification for DNS over Transport Layer Security (TLS)".

[84] RFC 8310: "Usage Profiles for DNS over TLS and DNS over DTLS".

[85] RFC 4890: "Recommendations for Filtering ICMPv6 Messages in Firewalls".

[86] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[87] 3GPP TS 38.305: "Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[88] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".

[89] IANA: "Transport Layer Security (TLS) Parameters".

[90] RFC 2818: "HTTP Over TLS".

[91] 3GPP TS 33.535: "Authentication and key management for applications based on 3GPP credentials in the 5G System (5GS)".

[92] 3GP TS 29.573: "5G System; Public Land Mobile Network (PLMN) Interconnection".

[93] 3GPP TS 29.503: "5G System; Unified Data Management Services".

[xx] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[yy] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**5G security context:** The state that is established locally at the UE and a serving network domain and represented by the "5G security context data" stored at the UE and a serving network.

NOTE 1: The "5G security context data" consists of the 5G NAS security context, and the 5G AS security context for 3GPP access and/or the 5G AS security context for non-3GPP access.

NOTE 2: A 5G security context has type "mapped", "full native" or "partial native". Its state can either be "current" or "non-current". A context can be of one type only and be in one state at a time. The state of a particular context type can change over time. A partial native context can be transformed into a full native. No other type transformations are possible.

**5G AS security context for 3GPP access:** The cryptographic keys at AS level with their identifiers, the Next Hop parameter (NH), the Next Hop Chaining Counter parameter (NCC) used for next hop access key derivation, the identifiers of the selected AS level cryptographic algorithms, the UE security capabilities, and the UP Security Policy at the network side, UP security activation status and the counters used for replay protection.

NOTE 3: NH and NCC need to be stored also at the AMF during connected mode.

NOTE 4: UP security activation status is sent from gNB/ng-eNB in step 1b in clause 6.6.2 corresponding to the active PDU session(s).

**5G AS security context for non-3GPP access:** The key KN3IWF, the cryptographic keys, cryptographic algorithms and tunnel security association parameters used at IPsec layer for the protection of IPsec SA.

**5G AS Secondary Cell security context**: The cryptographic keys at AS level for secondary cell with their identifiers, the identifier of the selected AS level cryptographic algorithms for secondary cell, the UP Security Policy at the network side, and counters used for replay protection.

**5G** **Home Environment Authentication Vector:** authentication data consisting of RAND, AUTN, XRES\*, and KAUSF for the purpose of authenticating the UE using 5G AKA.

NOTE 3a: This vector is received by the AUSF from the UDM/ARPF in the Nudm\_Authentication\_Get Response.

**5G Authentication Vector:** authentication data consisting of RAND, AUTN, HXRES\*, and KSEAF.

NOTE 3b: This vector is received by the SEAF from the AUSF in the Nausf\_Authentication\_Authenticate Response.

**5G NAS security context:** The key KAMF with the associated key set identifier, the UE security capabilities, the uplink and downlink NAS COUNT values.

NOTE 4: The distinction between native 5G security context and mapped 5G security context also applies to 5G NAS security contexts. The 5G NAS security context is called "full" if it additionally contains the integrity and encryption keys and the associated identifiers of the selected NAS integrity and encryption algorithms.

**5G Serving Environment Authentication Vector:** a vector consisting of RAND, AUTN and HXRES\*.

**ABBA parameter:** Parameter that provides antibidding down protection of security features against security features introduced in higher release to a lower release and indicates the security features that are enabled in the current network.

**activation of security context:** The process of taking a security context into use.

**anchor key:** The security key KSEAF provided during authentication and used for derivation of subsequent security keys.

**application Layer Security:** mechanism by which HTTP messages, exchanged between a Network Function in one PLMN and a Network Function in another PLMN, are protected on the N32-f interface between the two SEPPs in the two PLMNs.

**authentication data:** An authentication vectoror transformed authentication vector.

**authentication vector:** A vector consisting of CK, IK, RAND, AUTN, and XRES.

**backward security**: The property that for an entity with knowledge of Kn, it is computationally infeasible to compute any previous Kn-m (m>0) from which Kn is derived.

NOTE 5: In the context of KgNB key derivation, backward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to compute any previous KgNB that has been used between the same UE and a previous gNB.

**CM-CONNECTED state:** This is as defined in TS 23.501 [2].

NOTE5a: The term CM-CONNECTED state corresponds to the term 5GMM-CONNECTED mode used in TS 24.501 [35].

**CM-IDLE state:** As defined in TS 23.501 [2].

NOTE5b: The term CM-IDLE state corresponds to the term 5GMM-IDLE mode used in TS 24.501 [35].

**consumer's IPX (cIPX):** IPX provider entity with a business relationship with the cSEPP operator.

**consumer's SEPP (cSEPP):** The SEPP residing in the PLMN where the service consumer NF is located.

**Credentials Holder:** As defined in TS 23.501 [2].

**current 5G security context:** The security context which has been activated most recently.

NOTE5c: A current 5G security context originating from either a mapped or native 5G security context can exist simultaneously with a native non-current 5G security context.

**Default Credentials Server:** As defined in TS 23.501[2].

**Default UE credentials:** As defined in TS 23.501[2].

**forward security**: The fulfilment of the property that for an entity with knowledge of Km that is used between that entity and a second entity, it is computationally infeasible to predict any future Km+n (n>0) used between a third entity and the second entity.

NOTE 6: In the context of KgNB key derivation, forward security refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to predict any future KgNB that will be used between the same UE and another gNB. More specifically, n hop forward security refers to the property that a gNB is unable to compute keys that will be used between a UE and another gNB to which the UE is connected after n or more handovers (n=1 or more).

**full native 5G security context:** A native 5G security context for which the 5G NAS security context is full according to the above definition.

NOTE6a: A full native 5G security context is either in state "current" or state "non-current".

**Home Network Identifier:** An identifier identifying the home network of the subscriber.

NOTE6b: Described in detail in TS 23.003 [19].

**Home Network Public Key Identifier:** An identifier used to indicate which public/private key pair is used for SUPI protection and de-concealment of the SUCI.

NOTE6c: Described in this document and detailed in TS 23.003 [19].

**IAB-donor-CU**: As defined in TS 38.401 [78] .

**IAB-donor-DU**: As defined in TS 38.401 [78].

**IAB-node**: As defined in TS 38.300 [52].

**IAB-donor gNB**:As defined in TS 38.300 [52].

**IAB-UE**: The function within an IAB node, which behaves as a UE.

**mapped 5G security context**: An 5G security context, whose KAMF was derived from EPS keys during interworking and which is identified by mapped ngKSI.

**Master node**: As defined in TS 37.340 [51].

**N32-c connection:** A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.

NOTE 6d: This is a short-lived connection that is used between the SEPPs for cipher suite and protection policy exchange, and error notifications.

**N32-f connection:** Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.

NOTE 6e: When IPX providers are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

**native 5G security context:** An 5G security context, whose KAMF was created by a run of primary authentication and which is identified by native ngKSI.

**ng-eNB**: As defined in TS 38.300 [52].

**NG-RAN node**: gNB or ng-eNB (as defined in TS 38.300 [52]).

**non-current 5G security context:** A native 5G security context that is not the current one.

NOTE 7: A non-current 5G security context may be stored along with a current 5G security context in the UE and the AMF. A non-current 5G security context does not contain 5G AS security context. A non-current 5G security context is either of type "full native" or of type "partial native".

**partial native 5G security context:** A partial native 5G security context consists of KAMF with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values, which are initially set to zero before the first NAS SMC procedure for this security context.

NOTE 8: A partial native 5G security context is created by primary authentication, for which no corresponding successful NAS SMC has been run. A partial native context is always in state "non-current".

**producer's IPX (pIPX)**: IPX provider entity with a business relationship with the pSEPP operator.

**producer's SEPP (pSEPP):** The SEPP residing in the PLMN where the service producer NF is located.

**Protection Scheme Identifier:** An identifier identifying a protection scheme that is used for concealing the SUPI.

**RM-DEREGISTERED state:** This is as defined in TS 23.501 [2].

NOTE8a: The term RM-DEREGISTERED state corresponds to the term 5GMM-DEREGISTERED mode used in TS 24.501 [35].

**RM-REGISTERED state:** As defined in TS 23.501 [2].

NOTE8b: The term RM-REGISTERED state corresponds to the term 5GMM-REGISTERED mode used in TS 24.501 [35].

**Routing Indicator:** An indicator defined in TS 23.003 [19] that can be used for AUSF or UDM selection.

**Scheme Output**: the output of a public key protection scheme used for SUPI protection.

**security anchor function:** The function SEAF that serves in the serving network as the anchor for security in 5G.

**Secondary node**: As defined in TS 37.340 [51].

**subscription credential(s):** The set of values in the USIM and in the home operator's network, consisting of at least the long-term key(s) and the subscription identifier SUPI, used to uniquely identify a subscription and to mutually authenticate the UE and 5G core network.

**subscription identifier:** The SUbscription Permanent Identifier (SUPI).

NOTE8c: As defined in TS 23.501 [2] and detailed in 23.003 [19].

**subscription concealed identifier:** A one-time use subscription identifier, called the SUbscription Concealed Identifier (SUCI), which contains the Scheme-Output, and additional non-concealed information needed for home network routing and protection scheme usage.

NOTE8d: Defined in the present document; detailed in TS 23.003 [19].

**subscription identifier de-concealing function:** The Subscription Identifier De-concealing Function (SIDF) service offered by the network function UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI.

**transformed authentication vector:** an authentication vector where CK and IK have been replaced with CK' and IK'.

**UE 5G security capability:** The UE security capabilities for 5G AS and 5G NAS.

**UE security capabilities:** The set of identifiers corresponding to the ciphering and integrity algorithms implemented in the UE.

NOTE 9: This includes capabilities for NG-RAN and 5G NAS, and includes capabilities for EPS, UTRAN and GERAN if these access types are supported by the UE.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core Network

5G-AN 5G Access Network

5G-RG 5G Residential Gateway

NG-RAN 5G Radio Access Network

5G AV 5G Authentication Vector

5G HE AV 5G Home Environment Authentication Vector

5G SE AV 5G Serving Environment Authentication Vector

ABBAAnti-Bidding down Between Architectures

AEAD Authenticated Encryption with Associated Data

AES Advanced Encryption Standard

AKA Authentication and Key Agreement

AMF Access and Mobility Management Function

AMF Authentication Management Field

NOTE: If necessary, the full word is spelled out to disambiguate the abbreviation.

ARPF Authentication credential Repository and Processing Function

AUSF Authentication Server Function

AUTN AUthentication TokeN

AV Authentication Vector

AV' transformed Authentication Vector

BAP Backhaul Adaptation Protocol

BH Backhaul

CCA Client Credentials Assertion

Cell-ID Cell Identity as used in TS 38.331 [22]

CH Credentials Holder

CHO Conditional Handover

CIoT Cellular Internet of Things

cIPX consumer's IPX

CKSRVCC Cipher Key for Single Radio Voice Continuity

CP Control Plane

cSEPP consumer's SEPP

CTR Counter (mode)

CU Central Unit

DCS Default Credentials Server

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

ENSI External Network Slice Inforamtion

EPS Evolved Packet System

FN-RG Fixed Network RG

gNB NR Node B

GUTI Globally Unique Temporary UE Identity

HRES Hash RESponse

HXRES Hash eXpected RESponse

IAB Integrated Access and Backhaul

IKE Internet Key Exchange

IKSRVCC Integrity Key for Single Radio Voice Continuity

IPUPS Inter-PLMN UP Security

IPX IP exchange service

KSI Key Set Identifier

KSISRVCC Key Set Identifier for Single Radio Voice Continuity

LI Lawful Intercept

MN Master Node

MO-EDT Mobile Originated Early Data Transmission

MT-EDT Mobile Terminated Early Data Transmission

MR-DC Multi-Radio Dual Connectivity

MSK Master Session Key

N3IWF Non-3GPP access InterWorking Function

NAI Network Access Identifier

NAS Non Access Stratum

NDS Network Domain Security

NEA Encryption Algorithm for 5G

NF Network Function

NG Next Generation

ng-eNB Next Generation Evolved Node-B

ngKSI Key Set Identifier in 5G

N5CW Non-5G-Capable over WLAN

N5GC Non-5G-Capable

NIA Integrity Algorithm for 5G

NR New Radio

NR-DC NR-NR Dual Connectivity

NSSAI Network Slice Selection Assistance Information

NSSAA Network Slice Specific Authentication and Authorization

PDN Packet Data Network

PEI Permanent Equipment Identifier

pIPX producer's IPX

PRINS PRotocol for N32 INterconnect Security

pSEPP producer's SEPP

PUR Preconfigured Uplink Resource

QoS Quality of Service

RES RESponse

SCG Secondary Cell Group

SEAF SEcurity Anchor Function

SCP Service Communication Proxy

NOTE: Void. Security Gateway

SEPP Security Edge Protection Proxy

SIDF Subscription Identifier De-concealing Function

SMC Security Mode Command

SMF Session Management Function

SN Secondary Node

SN Id Serving Network Identifier

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TLS Transport Layer Security

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TWAP Trusted WLAN Access Point

TWIF Trusted WLAN Interworking Function

TSC Time Sensitive Communication

UE User Equipment

UEA UMTS Encryption Algorithm

UDM Unified Data Management

UDR Unified Data Repository

UIA UMTS Integrity Algorithm

ULR Update Location Request

UP User Plane

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

USIM Universal Subscriber Identity Module

XRES eXpected RESponse

\*\*\* 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 SNPN ID of the serving SNPN is included instead of the serving PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the home PLMN ID.

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 SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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 SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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 SNPN ID of the serving SNPN is included instead of the NF Service Consumer's PLMN ID and the SNPN ID or the PLMN ID of the Credentials Holder is included instead of the NF Service Producer's PLMN ID.

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 SNPN ID of the serving SNPN contained in the API request instead of the PLMN-ID, and the SNPN ID or the PLMN ID of the Credentials Holder instead of the home PLMN ID.

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 or EAP-TTLS inner method messages towards a AAA Server and performing related protocol conversion as needed. **Input, Required:**

1) In EAP Authentication:

a) In the initial authentication request: SUPI.

b) In subsequent authentication requests: EAP message.

2) In case EAP-TTLS mechanisms are implemented: inner method container.

**Input, Optional:** None

**Output, Required:**

1) In EAP authentication: EAP message, authentication result and if success MSK and SUPI.

2) In case EAP-TTLS mechanisms are implemented: inner method container.

**Output, Optional:** None

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

Annex X (informative):  
Primary authentication using EAP-TTLS in SNPNs

X.1 Introduction

In SNPN, when a credential holder is located outside of the 5GC of the SNPN, EAP-TTLS can be used to authenticate the UE. EAP-TTLS consists of two phases of authentication. In the first phase, a TLS tunnel is established between the UE and the EAP-TTLS server on AUSF. In the second phase, a legacy authentication protocol can be run between the UE and the credential holder (namely AAA) through the established TLS tunnel.

After the successful completion of EAP-TTLS, the AUSF and the UE derive the KAUSF from the EMSK.

UE is provisioned with a trust anchor to enable verification of the EAP-TTLS server certificate. The provisioning of trust anchor on the UE is outside the scope of this document.

X.2 Procedure



**Figure: X.2-1: Primary authentication using EAP-TTLS and AAA**

0. The UE is configured with the trust anchor needed to authenticate the certificate of the EAP-TTLS server running on the AUSF. Further, the UE is configured with the credentials required to authenticate with the AAA server.

Steps 1-17 are same as the steps 1-17 in clause B.2.2.1 in Annex B, except in the following steps:

1. The SUPI in the NAI format, i.e., username@realm, is used.

5. EAP-TTLS is selected by the UDM as the authentication method.

6-17. EAP-TTLS phase 1 is executed between the AUSF and the UE. EAP-Type is set to EAP-TTLS and the authentication of the UE using TLS client certificate is skipped. Since TLS client certificate is not used in EAP-TTLS, the UE need not be configured with UE certificate.

18-27. After EAP-TTLS phase 1 is successfully completed, the UE runs EAP-TTLS phase 2 authentication with the AAA as specified in RFC 5281 [XX] via NSSAAF. The phase 2 authentication method used is outside the scope of the present document but MS-CHAPv2 is depicted here as an example to show that the Nnssaaf\_AIW\_Authentication service offered by NSSAAF carries AVPs if the phase 2 authentication method is non-EAP.

NOTE: As referenced in section 14.1.11 of RFC 5281 [XX], allowing the use of phase 2 (inner) authentication method outside of tunnelled protocol leads to Man-in-the-Middle (MitM) vulnerability. Thus, it is assumed that the UE does not allow the use of phase 2 authentication method outside of TLS tunnel (i.e., the UE does not respond to requests for phase 2 authentication outside of the TLS tunnel). In environments where the use of phase 2 authentication outside of the tunnelled protocol cannot be prevented, EAP-TTLS implementations need to address this vulnerability by using EAP channel binding or cryptographic binding described in RFC 6678 [YY].

28-31. After EAP-TTLS phase 2 authentication is successfully completed, the rest of the procedures are same as steps 18- 21 described in clause B.2.1.1, except that the EAP-Type is set to EAP-TTLS in the EAP Response message from the UE to the AUSF.

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