**3GPP TSG-WG SA2 Meeting #139E e-meeting  *S2-2003743***

**Elbonia, June 1 – 5, 2020 (Phase-1) (revision of S2-200xxxx)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.501** | **CR** | **2372** | **rev** | **-** | **Current version:** | **16.4.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Replacing AUSF by NSSAAF to support NSSAA | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | ZTE?, Ericsson?, Qualcomm?, Nokia?, Nokia shanghai Bell?, Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNS | | | | |  | ***Date:*** | | | 2020-05-10 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | After thorough analysis, SA3 has decided on the security requirement to fully isolate the following two SBA Authentication service types,   * primary authentication services towards UDM currently supported by AUSF * NSSAA services involving interactions with a AAA-S   As a result, the NSSAA SBI services used by the AMF shall be hosted by a new NF, i.e. NSSAA Function (NSSAAF), to provide the NSSAA related services. From a specification point of view, this will require the definition of a new NF within the SBA architecture. From AMF point of view, this requires that AMF selects the new NF in the HPLMN when an NSSAA service is invoked.  According to the last e-meeting discussion, the UE may no longer access to the authorized S-NSSAIs due to, e.g., Deregistration or 5GS to EPS mobility in which case the PDU sessions associated with S-NSSAIs subject to NSSAA cannot be maintained. However, there is no corresponding method of how to terminate the notification of re-authentication and re-authorization or revocation from AAA-S via the newly defined NSSAAF, hence the AAA server will keep notify AMF on the re-authorization or Revocation even after UE don’t use the slice any more.  It is proposed that the AMF unsubscribes the notification of Re-authentication and Re-authorization or Revocation via the NSSAAF (see Fourth Change). | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Introducing the new NF, NSSAAF, into Rel-17 network architecture to replace AUSF to support NSSAA by adding/updating the corresponding clauses to support this new NF. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Fail to align the stage-2 architecture and solutions with stage-3 for Rel-16 to support network slice specific authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.2, 4.2.2, 4.2.3, 4.2.4, 4.2.6, 4.2.7, 6.2.8, 6.2.X, 7.2.7, 7.2.X | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\* \* \* \* First change \* \* \* \*

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

5GC 5G Core Network

5GLAN 5G Local Area Network

5GS 5G System

5G-AN 5G Access Network

5G-AN PDB 5G Access Network Packet Delay Budget

5G-EIR 5G-Equipment Identity Register

5G-GUTI 5G Globally Unique Temporary Identifier

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5G GM 5G Grand Master

5G-RG 5G Residential Gateway

5G-S-TMSI 5G S-Temporary Mobile Subscription Identifier

5G VN 5G Virtual Network

5QI 5G QoS Identifier

AF Application Function

AMF Access and Mobility Management Function

AS Access Stratum

ATSSS Access Traffic Steering, Switching, Splitting

ATSSS-LL ATSSS Low-Layer

AUSF Authentication Server Function

BMCA Best Master Clock Algorithm

BSF Binding Support Function

CAG Closed Access Group

CAPIF Common API Framework for 3GPP northbound APIs

CHF Charging Function

CN PDB Core Network Packet Delay Budget

CP Control Plane

DL Downlink

DN Data Network

DNAI DN Access Identifier

DNN Data Network Name

DRX Discontinuous Reception

DS-TT Device-side TSN translator

ePDG evolved Packet Data Gateway

EBI EPS Bearer Identity

EUI Extended Unique Identifier

FAR Forwarding Action Rule

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

FN-RG Fixed Network RG

FQDN Fully Qualified Domain Name

GFBR Guaranteed Flow Bit Rate

GMLC Gateway Mobile Location Centre

GPSI Generic Public Subscription Identifier

GUAMI Globally Unique AMF Identifier

HR Home Routed (roaming)

IAB Integrated access and backhaul

IMEI/TAC IMEI Type Allocation Code

IPUPS Inter PLMN UP Security

I-SMF Intermediate SMF

I-UPF Intermediate UPF

LADN Local Area Data Network

LBO Local Break Out (roaming)

LMF Location Management Function

LoA Level of Automation

LPP LTE Positioning Protocol

LRF Location Retrieval Function

MCX Mission Critical Service

MDBV Maximum Data Burst Volume

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

MPS Multimedia Priority Service

MPTCP Multi-Path TCP Protocol

N3IWF Non-3GPP InterWorking Function

N5CW Non-5G-Capable over WLAN

NAI Network Access Identifier

NEF Network Exposure Function

NF Network Function

NGAP Next Generation Application Protocol

NID Network identifier

NPN Non-Public Network

NR New Radio

NRF Network Repository Function

NSI ID Network Slice Instance Identifier

NSSAA Network Slice-Specific Authentication and Authorization

NSSAAF Network Slice-Specific Authentication and Authorization Function

NSSAI Network Slice Selection Assistance Information

NSSF Network Slice Selection Function

NSSP Network Slice Selection Policy

NW-TT Network-side TSN translator

NWDAF Network Data Analytics Function

PCF Policy Control Function

PDB Packet Delay Budget

PDR Packet Detection Rule

PDU Protocol Data Unit

PEI Permanent Equipment Identifier

PER Packet Error Rate

PFD Packet Flow Description

PNI-NPN Public Network Integrated Non-Public Network

PPD Paging Policy Differentiation

PPF Paging Proceed Flag

PPI Paging Policy Indicator

PSA PDU Session Anchor

PTP Precision Time Protocol

QFI QoS Flow Identifier

QoE Quality of Experience

RACS Radio Capabilities Signalling optimisation

(R)AN (Radio) Access Network

RG Residential Gateway

RIM Remote Interference Management

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSN Redundancy Sequence Number

SA NR Standalone New Radio

SBA Service Based Architecture

SBI Service Based Interface

SCP Service Communication Proxy

SD Slice Differentiator

SEAF Security Anchor Functionality

SEPP Security Edge Protection Proxy

SMF Session Management Function

SMSF Short Message Service Function

SN Sequence Number

SNPN Stand-alone Non-Public Network

S-NSSAI Single Network Slice Selection Assistance Information

SSC Session and Service Continuity

SSCMSP Session and Service Continuity Mode Selection Policy

SST Slice/Service Type

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

SV Software Version

TNAN Trusted Non-3GPP Access Network

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TNL Transport Network Layer

TNLA Transport Network Layer Association

TSC Time Sensitive Communication

TSCAI TSC Assistance Information

TSN Time Sensitive Networking

TSN GM TSN Grand Master

TSP Traffic Steering Policy

TT TSN Translator

TWIF Trusted WLAN Interworking Function

UCMF UE radio Capability Management Function

UDM Unified Data Management

UDR Unified Data Repository

UDSF Unstructured Data Storage Function

UL Uplink

UL CL Uplink Classifier

UPF User Plane Function

URLLC Ultra Reliable Low Latency Communication

URRP-AMF UE Reachability Request Parameter for AMF

URSP UE Route Selection Policy

VID VLAN Identifier

VLAN Virtual Local Area Network

W-5GAN Wireline 5G Access Network

W-5GBAN Wireline BBF Access Network

W-5GCAN Wireline 5G Cable Access Network

W-AGF Wireline Access Gateway Function

\* \* \* \* Second change \* \* \* \*

### 4.2.2 Network Functions and entities

The 5G System architecture consists of the following network functions (NF).

- Authentication Server Function (AUSF)

- Access and Mobility Management Function (AMF)

- Data Network (DN), e.g. operator services, Internet access or 3rd party services

- Unstructured Data Storage Function (UDSF)

- Network Exposure Function (NEF)

- Intermediate NEF (I-NEF)

- Network Repository Function (NRF)

- Network Slice Specific Authentication and Authorization Function (NSSAAF)

- Network Slice Selection Function (NSSF)

- Policy Control Function (PCF)

- Session Management Function (SMF)

- Unified Data Management (UDM)

- Unified Data Repository (UDR)

- User Plane Function (UPF)

- UE radio Capability Management Function (UCMF)

- Application Function (AF)

- User Equipment (UE)

- (Radio) Access Network ((R)AN)

- 5G-Equipment Identity Register (5G-EIR)

- Network Data Analytics Function (NWDAF)

- CHarging Function (CHF)

NOTE: The functional description of the CHF is specified in TS 32.240 [41].

The 5G System architecture also comprises the following network entities:

- Service Communication Proxy (SCP)

- Security Edge Protection Proxy (SEPP)

The functional descriptions of these Network Functions and entities are specified in clause 6.

- Non-3GPP InterWorking Function (N3IWF)

- Trusted Non-3GPP Gateway Function (TNGF)

- Wireline Access Gateway Function (W-AGF)

- Trusted WLAN Interworking Function (TWIF)

### 4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.



Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

Figure 4.2.3-2 depicts the 5G System architecture in the non-roaming case, using the reference point representation showing how various network functions interact with each other.



NOTE 1: N9, N14 are not shown in all other figures however they may also be applicable for other scenarios.

NOTE 2: For the sake of clarity of the point-to-point diagrams, the UDSF, NEF and NRF have not been depicted. However, all depicted Network Functions can interact with the UDSF, UDR, NEF and NRF as necessary.

NOTE 3: The UDM uses subscription data and authentication data and the PCF uses policy data that may be stored in UDR (refer to clause 4.2.5).

NOTE 4: For clarity, the UDR and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on data storage architectures refer to clause 4.2.5.

NOTE 5: For clarity, the NWDAF and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on network data analytics architecture refer to TS 23.288 [86].

Figure 4.2.3-2: Non-Roaming 5G System Architecture in reference point representation

Figure 4.2.3-3 depicts the non-roaming architecture for UEs concurrently accessing two (e.g. local and central) data networks using multiple PDU Sessions, using the reference point representation. This figure shows the architecture for multiple PDU Sessions where two SMFs are selected for the two different PDU Sessions. However, each SMF may also have the capability to control both a local and a central UPF within a PDU Session.



Figure 4.2.3-3: Applying non-roaming 5G System architecture for multiple PDU Session in reference point representation

Figure 4.2.3-4 depicts the non-roaming architecture in the case of concurrent access to two (e.g. local and central) data networks is provided within a single PDU Session, using the reference point representation.



Figure 4.2.3-4: Applying non-roaming 5G System architecture for concurrent access to two (e.g. local and central) data networks (single PDU Session option) in reference point representation

Figure 4.2.3-5 depicts the non-roaming architecture for Network Exposure Function, using reference point representation.



Figure 4.2.3-5: Non-roaming architecture for Network Exposure Function in reference point representation

NOTE 1: In figure 4.2.3-5, Trust domain for NEF is same as Trust domain for SCEF as defined in TS 23.682 [36].

NOTE 2: In figure 4.2.3-5, 3GPP Interface represents southbound interfaces between NEF and 5GC Network Functions e.g. N29 interface between NEF and SMF, N30 interface between NEF and PCF, etc. All southbound interfaces from NEF are not shown for the sake of simplicity.

### 4.2.4 Roaming reference architectures

Figure 4.2.4-1 depicts the 5G System roaming architecture with local breakout with service-based interfaces within the Control Plane.



Figure 4.2.4-1: Roaming 5G System architecture- local breakout scenario in service-based interface representation

NOTE 1: In the LBO architecture. The PCF in the VPLMN may interact with the AF in order to generate PCC Rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation. The PCF in VPLMN has no access to subscriber policy information from the HPLMN.

NOTE 2: An SCP can be used for indirect communication between NFs and NF services within theVPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

Figure 4.2.4-3 depicts the 5G System roaming architecture in the case of home routed scenario with service-based interfaces within the Control Plane.



Figure 4.2.4-3: Roaming 5G System architecture - home routed scenario in service-based interface representation

NOTE 3: An SCP can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

NOTE 4: UPFs in the home routed scenario can be used also to support the IPUPS functionality (see clause 5.8.2.14).

Figure 4.2.4-4 depicts 5G System roaming architecture in the case of local break out scenario using the reference point representation.



Figure 4.2.4-4: Roaming 5G System architecture - local breakout scenario in reference point representation

NOTE 5: The NRF is not depicted in reference point architecture figures. Refer to Figure 4.2.4-7 for details on NRF and NF interfaces.

NOTE 6: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

The following figure 4.2.4-6 depicts the 5G System roaming architecture in the case of home routed scenario using the reference point representation.



Figure 4.2.4-6: Roaming 5G System architecture - Home routed scenario in reference point representation

For the roaming scenarios described above each PLMN implements proxy functionality to secure interconnection and hide topology on the inter-PLMN interfaces.



Figure 4.2.4-7: NRF Roaming architecture in reference point representation

NOTE 7: For the sake of clarity, SEPPs on both sides of PLMN borders are not depicted in figure 4.2.4-7.

In roaming scenarios, the I-NEF may be deployed. The I-NEF is described in clause 6.2.5a. Figure 4.2.4-8 depicts the roaming architecture for Network Exposure Function, using reference point representation.



Figure 4.2.4-8: Roaming architecture for Network Exposure Function in reference point representation

NOTE 8: The reference architecture in figure 4.2.4-8 supports service based interfaces on the I-NEF.

Operators can deploy UPFs supporting the Inter PLMN UP Security (IPUPS) functionality at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios. The UPFs supporting the IPUPS functionality in VPLMN and HPLMN are controlled by the V-SMF and the H-SMF of that PDU Session respectively. A UPF supporting the IPUPS functionality terminates GTP-U N9 tunnels. The SMF can activate the IPUPS functionality together with other UP functionality in the same UPF, or insert a separate UPF for the IPUPS functionality in the UP path (which e.g. may be dedicated to be used for IPUPS functionality). Figure 4.2.4-9 depicts the home routed roaming architecture where a UPF is inserted in the UP path for the IPUPS functionality. Figure 4.2.4-3 depicts the home routed roaming architecture where the two UPFs perform the IPUPS functionality and other UP functionality for the PDU Session.

NOTE 9: Operators are not prohibited from deploying the IPUPS functionality as a separate Network Function from the UPF, acting as a transparent proxy which can transparently read N4 and N9 interfaces. However, such deployment option is not specified and needs to take at least into account very long lasting PDU Sessions with infrequent traffic and Inter-PLMN handover.

The IPUPS functionality is specified in clause 5.8.2.14 and TS 33.501 [29].



Figure 4.2.4-9: Roaming 5G System architecture - home routed roaming scenario in service-based interface representation employing UPF dedicated to IPUPS

\* \* \* \* Third change \* \* \* \*

### 4.2.6 Service-based interfaces

The 5G System Architecture contains the following service-based interfaces:

**Namf:** Service-based interface exhibited by AMF.

**Nsmf:** Service-based interface exhibited by SMF.

**Nnef:** Service-based interface exhibited by NEF.

**Npcf:** Service-based interface exhibited by PCF.

**Nudm:** Service-based interface exhibited by UDM.

**Naf:** Service-based interface exhibited by AF.

**Nnrf:** Service-based interface exhibited by NRF.

**Nnssaaf:** Service-based interface exhibited by NSSAAF.

**Nnssf**: Service-based interface exhibited by NSSF.

**Nausf:** Service-based interface exhibited by AUSF.

**Nudr:** Service-based interface exhibited by UDR.

**Nudsf:** Service-based interface exhibited by UDSF.

**N5g-eir:** Service-based interface exhibited by 5G-EIR.

**Nnwdaf:** Service-based interface exhibited by NWDAF.

**Ni-nef:** Service-based interface exhibited by I-NEF.

**Nchf:** Service-based interface exhibited by CHF.

**Nucmf:** Service-based interface exhibited by UCMF.

NOTE: The Service-based interface exhibited by CHF is defined in TS 32.240 [41].

### 4.2.7 Reference points

The 5G System Architecture contains the following reference points:

**N1:** Reference point between the UE and the AMF.

**N2:** Reference point between the (R)AN and the AMF.

**N3:** Reference point between the (R)AN and the UPF.

**N4:** Reference point between the SMF and the UPF.

**N6:** Reference point between the UPF and a Data Network.

NOTE 1: The traffic forwarding details of N6 between a UPF acting as an uplink classifier and a local data network are not specified in this Release of the specification.

**N9:** Reference point between two UPFs.

The following reference points show the interactions that exist between the NF services in the NFs. These reference points are realized by corresponding NF service-based interfaces and by specifying the identified consumer and producer NF service as well as their interaction in order to realize a particular system procedure.

**N5:** Reference point between the PCF and an AF.

**N7:** Reference point between the SMF and the PCF.

**N8:** Reference point between the UDM and the AMF.

**N10:** Reference point between the UDM and the SMF.

**N11:** Reference point between the AMF and the SMF.

**N12:** Reference point between AMF and AUSF.

**N13:** Reference point between the UDM and Authentication Server function the AUSF.

**N14:** Reference point between two AMFs.

**N15:** Reference point between the PCF and the AMF in the case of non-roaming scenario, PCF in the visited network and AMF in the case of roaming scenario.

**N16:** Reference point between two SMFs, (in roaming case between SMF in the visited network and the SMF in the home network).

**N16a:** Reference point between SMF and I-SMF.

**N17:** Reference point between AMF and 5G-EIR.

**N18:** Reference point between any NF and UDSF.

**N19:** Reference point between two PSA UPFs for 5G LAN-type service.

**N22:** Reference point between AMF and NSSF.

**N23:** Reference point between PCF and NWDAF.

**N24:** Reference point between the PCF in the visited network and the PCF in the home network.

**N27:** Reference point between NRF in the visited network and the NRF in the home network.

**N28:** Reference point between PCF and CHF.

**N29:** Reference point between NEF and SMF.

**N29i:** Reference point between I-NEF and SMF in the VPLMN.

**N30:** Reference point between PCF and NEF.

NOTE 2: The functionality of N28 and N29 and N30 reference points are defined in TS 23.503 [45].

**N31:** Reference point between the NSSF in the visited network and the NSSF in the home network.

NOTE 3: in some cases, a couple of NFs may need to be associated with each other to serve a UE.

In addition to the reference points above, there are interfaces/reference point(s) between SMF and the CHF. The reference point(s) are not depicted in the architecture illustrations in this specification.

NOTE 4: The functionality of these interface/reference points are defined in TS 32.240 [41].

**N32:** Reference point between SEPP in the visited network and the SEPP in the home network.

NOTE 5: The functionality of N32 reference point is defined in TS 33.501 [29].

**N33:** Reference point between NEF and AF.

**N34:** Reference point between NSSF and NWDAF.

**N35:** Reference point between UDM and UDR.

**N36:** Reference point between PCF and UDR.

**N37:** Reference point between NEF and UDR.

**N38:** Reference point between I-SMFs.

**N40:** Reference point between SMF and the CHF.

NOTE 6: The reference points from N40 up to and including N49 are reserved for allocation and definition in TS 23.503 [45].

**N50:** Reference point between AMF and the CBCF.

**N51:** Reference point between AMF and NEF.

**N51i:** Reference point between I-NEF and the AMF in the VPLMN.

**N52:** Reference point between NEF and UDM.

**N53:** Reference point between the I-NEF and the NEF.

**N55:** Reference point between AMF and the UCMF.

**N56:** Reference point between NEF and the UCMF.

**N57:** Reference point between AF and the UCMF.

NOTE 7: The Public Warning System functionality of N50 reference point is defined in TS 23.041 [46].

**N58:** Reference point between AMF and the NSSAAF.

**N59:** Reference point between UDM and the NSSAAF.

The reference points to support SMS over NAS are listed in clause 4.4.2.2.

The reference points to support Location Services are listed in TS 23.273 [87].

The reference points to support SBA in IMS (N5, N70 and N71) are described in TS 23.228 [15].

\* \* \* \* Fourth change \* \* \* \*

### 5.15.10 Network Slice-Specific Authentication and Authorization

A serving PLMN shall perform Network Slice-Specific Authentication and Authorization for the S-NSSAIs of the HPLMN which are subject to it based on subscription information. The UE shall indicate in the Registration Request message in the UE 5GMM Core Network Capability whether it supports NSSAA feature. If the UE does not support NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, the AMF shall not trigger this procedure for the UE and they are rejected for the PLMN. If the UE supports NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, they are included in the list of Pending NSSAI for the PLMN, as described in clause 5.15.5.2.1.

If a UE is configured with S-NSSAIs, which are subject to Network Slice-Specific Authentication and Authorization, the UE stores an association between the S-NSSAI and corresponding credentials for the Network Slice-Specific Authentication and Authorization.

NOTE: The credentials for Network Slice-Specific Authentication and Authorization and how to provision them in the UE are not specified.

To perform the Network Slice-Specific Authentication and Authorization for an S-NSSAI, the AMF invokes an EAP- based Network Slice-Specific authorization procedure documented in TS 23.502 [3] clause 4.2.9 (see also TS 33.501 [29]) for the S-NSSAI. When an NSSAA procedure is started and is ongoing for an S-NSSAI, the AMF stores the NSSAA status of the S-NSSAI as pending, the NSSAA status of each S-NSSAI, if any is stored, is transferred when the AMF changes.

This procedure can be invoked for a supporting UE by an AMF at any time, e.g. when:

a. The UE registers with the AMF and one of the S-NSSAIs of the HPLMN which maps to an S-NSSAI in the Requested NSSAI is requiring Network Slice-Specific Authentication and Authorization (see clause 5.15.5.2.1 for details), and can be added to the Allowed NSSAI by the AMF once the Network Slice-Specific Authentication and Authorization for the S-NSSAI succeeds; or

b. The Network Slice-Specific AAA Server triggers a UE re-authentication and re-authorization for an S-NSSAI; or

c. The AMF, based on operator policy or a subscription change, decides to initiate the Network Slice-Specific Authentication and Authorization procedure for a certain S-NSSAI which was previously authorized.

In the case of re-authentication and re-authorization (b. and c. above) the following applies:

- If S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization are included in the Allowed NSSAI for each Access Type, AMF selects an Access Type to be used to perform the Network Slice Specific Authentication and Authorization procedure based on network policies.

- If the Network Slice-Specific Authentication and Authorization for some S-NSSAIs in the Allowed NSSAI is unsuccessful, the AMF shall update the Allowed NSSAI for each Access Type to the UE via UE Configuration Update procedure.

- If the Network Slice-Specific Authentication and Authorization fails for all S-NSSAIs in the Allowed NSSAI, the AMF shall execute the Network-initiated Deregistration procedure described in TS 23.502 [3], clause 4.2.2.3.3, and shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

After a successful or unsuccessful UE Network Slice-Specific Authentication and Authorization, the UE context in the AMF shall retain the authentication and authorization status for the UE for the related specific S-NSSAI of the HPLMN while the UE remains RM-REGISTERED in the PLMN, so that the AMF is not required to execute a Network Slice-Specific Authentication and Authorization for a UE at every Periodic Registration Update or Mobility Registration procedure with the PLMN.

A Network Slice-Specific AAA server may revoke the authorization or challenge the authentication and authorization of a UE at any time. When authorization is revoked for an S-NSSAI that is in the current Allowed NSSAI for an Access Type, the AMF shall provide a new Allowed NSSAI to the UE and trigger the release of all PDU sessions associated with the S-NSSAI, for this Access Type.

The AMF provides the GPSI of the UE related to the S-NSSAI to the AAA Server to allow the AAA server to initiate the Network Slice-Specific Authentication and Authorization, or the Authorization revocation procedure, where the current AMF serving the UE needs to be identified by the system, so the UE authorization status can be challenged or revoked.

The Network Slice-Specific Authentication and Authorization requires that the UE Primary Authentication and Authorization of the SUPI has successfully completed. If the SUPI authorization is revoked, then also the Network Slice-Specific authorization is revoked.

If the AMF determines that the UE no longer accesses the S-NSSAIs that map to the HPLMN S-NSSAIs for which Network Slice-Specific Authentication and Authorization succeeded previously, e.g. based on Deregistration or 5GS to EPS mobility, the AMF unsubscribes the notification of Re-authentication and Re-authorization or Revocation for the Network Slices identified by the HPLMN S-NSSAIs, as described in the clause 4.2.9.X in TS 23.502[3].

\* \* \* \* Fifth change \* \* \* \*

### 6.2.8 AUSF

The Authentication Server Function (AUSF) supports the following functionality:

- Supports authentication for 3GPP access and untrusted non-3GPP access as specified in TS 33.501 [29].

\* \* \* \* Sixth change \* \* \* \*

### 6.2.X NSSAAF

The Network Slice Specific Authentication and Authorization Function (NSSAAF) supports the following functionality:

- Support for Network Slice-Specific Authentication and Authorization as specified in TS 23.502 [3] with a AAA Server (AAA-S). If the AAA-S belongs to a third party, the NSSAAF may contact the AAA-S via an a AAA proxy ( AAA-P)

\* \* \* \* Seventh change \* \* \* \*

### 6.3.X NSSAAF discovery and selection

In the case of NF consumer based discovery and selection, the following applies:

- The AMF performs NSSAAF selection to select an NSSAAF Instance that supports network slice specific authentication between the UE and the AAA-S associated with the HPLMN. The AMF shall utilize the NRF to discover the NSSAAF instance(s) unless NSSAAF information is available by other means, e.g. locally configured on AMF. The NSSAAF selection function in the AMF selects an NSSAAF instance based on the available NSSAAF instances (obtained from the NRF or locally configured in the AMF).

NSSAAF selection is applicable to both 3GPP access and non-3GPP access.

The NSSAAF selection function in NSSAAF NF consumers or in SCP should consider the following factor when it is available:

1. Home Network Identifier (e.g., MNC and MCC) of SUPI (by an NF consumer in the Serving network) along with NID (when provided by the NG-RAN) in the case of SNPN.

NOTE 1: In the case of SNPN, the AMF uses the NID provided by the NG-RAN together with the selected PLMN ID (from SUCI/SUPI) as the SUCI/SUPI does not always include the NID.

In the case of delegated discovery and selection in SCP, the NSSAAF NF consumer shall send all available factors to the SCP.

\* \* \* \* Eighth change \* \* \* \*

### 7.2.7 AUSF Services

The following NF services are specified for AUSF:

Table 7.2.7-1: NF Services provided by AUSF

| Service Name | Description | Reference in TS 23.502 [3] |
| --- | --- | --- |
| Nausf UEauthentication | The AUSF provides UE authentication service to requester NF. For AKA based authentication, this operation can also be used to recover from security context synchronization failure situations. | 5.2.10.2 |
| Nausf\_SoRProtection | The AUSF provides protection of Steering of Roaming information service to the requester NF. | 5.2.10.3 |

\* \* \* \* Ninth change \* \* \* \*

### 7.2.X NSSAAF Services

The following NF services are specified for NSSAAF:

Table 7.2.X -1: NF Services provided by NSSAAF

| Service Name | Description | Reference in TS 23.502 [3] |
| --- | --- | --- |
| Nnssaaf\_NSSAA | The NSSAAF provides NSSAA service to the requester NF by relaying EAP messages towards a AAA-S or AAA-P and performing related protocol conversion as needed. It also provides notification to the current AMF where the UE is of the need to re-authenticate and re-authorize the UE or to revoke the UE authorization. | 5.2.10.5 |

\* \* \* \* End of changes \* \* \* \*