**3GPP TSG-SA3 Meeting #100e *S3-201817r1***

**e-meeting, 17 -28 August 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **0913** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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:*** | Editorial changes to Clause 16 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNS | | | | |  | ***Date:*** | | | 10/8/2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | R16 |
|  | *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:*** | | There are typos and misleading sentences to be updated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Editorial changes to the clause 16 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not clear or ambiguous NSSAA procedure | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 16 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **n** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **n** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **n** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 16 Security procedures for network slices

## 16.1 General

This clause specifies the security procedures for network slices.

## 16.2 Authorization for network slice access

This clause specifies the relationship between primary authentication (as described in Clause 6.1) and authorization for network slice access (as described in TS 23.502 [8]) for a UE. Authorization from a home/serving PLMN is required for a UE to gain access to a network slice, identified by an S-NSSAI. An authorized S-NSSAI (i.e. allowed S-NSSAI) shall be granted to a UE only after the UE has completed successfully primary authentication. At the end of the primary authentication, the AMF and UE may receive a list of allowed S-NSSAI, which the UE is authorized to access.

For certain S-NSSAIs, additional Network Slice Specific Authentication and Authorization (NSSAA) is required. This clause in addition specifies the pre-requisite for an NSSAA procedure that is described in clause 16.3, with reference to the following figure 16.2-1.



Figure 16.2-1: Relationship between primary authentication and NSSAA

1. UE sends a Registration Request with a list of S-NSSAIs. UE shall not include those S-NSSAIs for which NSSAA procedures are ongoing, regardless of access types (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2).

2. For an initial Registration Request, the AMF/SEAF shall invoke Primary authentication as described in clause 6.1.2 of the present document. For a subsequent Registration Request, the Primary authentication may be skipped if the UE has already been authenticated and the AMF has valid security context.

3. AMF shall determine whether NSSAA is required for each of S-NSSAIs, based on information stored locally or from UDM. For example, the NSSAA for an S-NSSAI may be omitted

1) if it is not required based on the subscription information,

2) if UE has previously performed NSSAA successfully, regardless of access type and the result is still valid, or

3) NSSAA for UE is ongoing

4. AMF sends the Registration Accept message to the UE (c.f. TS 23.501[2], clause 5.15.5.2.1 and TS 23.502[8], clause 4.2.2.2.2, step 21). Optionally UE sends a Registration Complete.

5. The EAP based NSSAA procedure for each S-NSSAI if required, as determined in step 3, is executed in this step.

6. Based on the results of step 5, AMF sends UE Configuration Update to update the requested S-NSSAI status based on the NSSAA results.

The procedure for step 5, i.e., the NSSAA procedure is specified in clause 16.3.

### 16.3 Network Slice specific authentication and authorization

This clause specifies the optional-to-use NSSAA between a UE and an AAA server (AAA-S) which may be owned by an external 3rd party enterprise. NSSAA uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication.

The EAP framework specified in RFC 3748 [27] shall be used for NSSAA between the UE and the AAA server. The SEAF/AMF shall perform the role of the EAP Authenticator and communicates with the AAA-S via the NSSAAF. The NSSAAF undertakes any AAA protocol interworking with the AAA-S. Multiple EAP methods are possible for NSSAA. If the AAA-S belongs to a third party the NSSAAF contacts the AAA-S via a AAA-P. The NSSAAF and the AAA-P maybe co-located.

To protect privacy of the EAP ID used for the EAP based NSSAA, a privacy-protection capable EAP method is recommended, if privacy protection is required.

The steps involved in NSSAA are described below.

**Figure 16.3-1: NSSAA procedure**

1. For S-NSSAIs that are requiring NSSAA, based on change of subscription information, or triggered by the AAA-S, the AMF may trigger the start of the NSSAA procedure.

If NSSAA is triggered as a result of Registration procedure, the AMF may determine, based on UE Context in the AMF, that for some or all S-NSSAI(s) subject to NSSAA, the UE has already been authenticated following a Registration procedure on a first access. Depending on NSSAA result (e.g. success/failure) from the previous Registration, the AMF may decide, based on Network policies, to skip NSSAA for these S-NSSAIs during the Registration on a second access.

If the NSSAA procedure corresponds to a re-authentication and re-authorization procedure triggered as a result of AAA Server-triggered UE re-authentication and re-authorization for one or more S-NSSAIs, as described in clause 4.2.9.2 of TS 23.502 [8], or triggered by the AMF based on operator policy or a subscription change and if S-NSSAIs that are requiring NSSAA are included in the Allowed NSSAI for each Access Type, the AMF selects an Access Type to be used to perform the NSSAA procedure based on network policies.

2. The AMF may request the UE User ID for EAP authentication (EAP ID) for the S-NSSAI in a NAS MM Transport message including the S-NSSAI.

3. The UE provides the EAP ID for the S-NSSAI alongside the S-NSSAI in an NAS MM Transport message towards the AMF.

4. The AMF sends the EAP ID to the NSSAAF which provides interface with the AAA, in an Nssaaf\_NSSAA\_Authenticate Request (EAP ID Response, GPSI, S-NSSAI).

5. If the AAA-P is present (e.g. because the AAA-S belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF forwards the EAP ID Response message to the AAA-P, otherwise the NSSAAF forwards the message directly to the AAA-S. NSSAAF routes to the AAA-S based on the S-NSSAI. The NSSAAF/AAA-P forwards the EAP Identity message to the AAA-S together with S-NSSAI and GPSI. The AAA-S stores the GPSI to create an association with the EAP ID in the EAP ID response message so the AAA-S can later use it to revoke authorisation or to trigger reauthentication. The AAA-S uses the EAP-ID and S-NSSAI to identify for which UE and slice authorisation is requested.

6 -11. EAP-messages are exchanged with the UE. One or more than one iterations of these steps may occur.

12. EAP authentication completes. An EAP-Success/Failure message is delivered to the NSSAAF/AAA-P along with GPSI and S-NSSAI.

13. The NSSAAF sends the Nssaaf\_NSSAA\_Authenticate Response (EAP-Success/Failure, S-NSSAI, GPSI) to the AMF.

14. The AMF transmits a NAS MM Transport message (EAP-Success/Failure) to the UE.

15. Based on the result of Slice specific authentication (EAP-Success/Failure), if a new Allowed NSSAI or new Rejected NSSAIs needs to be delivered to the UE, or if the AMF re-allocation is required, the AMF initiates the UE Configuration Update procedure, for each Access Type, as described in clause 4.2.4.2 of TS 23.502 [8].

Editor’s Note: It is ffs whether S-NSSAIs can be sent to AAA-S.

## 16.4 AAA Server triggered Network Slice-Specific Re-authentication and Re-authorization procedure

Figure 16.4-1: AAA Server initiated Network Slice-Specific Re-authentication and Re-authorization procedure

0. The UE is registered in 5GC via an AMF. The AMF ID is stored in the UDM.

1. The AAA-S requests the re-authentication and re-authorization for the Network Slice specified by the S-NSSAI in the Re-Auth Request message, for the UE identified by the GPSI in this message. This message is sent to an AAA-P, if the AAA-P is used (e.g. the AAA Server belongs to a third party), otherwise it may be sent directly to the NSSAAF. If an AAA-P is present, the AAA-P relays the Reauthentication Request to the NSSAAF.

2. The NSSAAF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE.

3. The NSSAAF requests the relevant AMF to re-authenticate/re-authorize the S-NSSAI for the UE using the Nssaaf\_NSSAA\_Re-authenticationNotification service operation. The AMF is implicitly subscribed to receive Nssaaf\_NSSAA\_Re-authenticationNotification service operations. The NSSAAF may discover the Callback URI for the Nssaaf\_NSSAA\_Re-authenticationNotification service operation exposed by the AMF via the NRF.

The AMF acknowledges the notification of Re-authentication request.

4. The AMF triggers the NSSAA procedure defined in clause 16.3 for the UE identified by the GPSI and the Network Slice identified by the S-NSSAI received from the NSSAAF.

## 16.5 AAA Server triggered Slice-Specific Authorization Revocation

Figure 16.5-1: AAA Server-initiated Network Slice-Specific Authorization Revocation procedure

0. The UE is registered in 5GC via an AMF. The AMF ID is stored in the UDM.

1. The slice specific AAA-S requests the revocation of authorization for the Network Slice identified by the GPSIin the AAA Protocol Revoke Authorization Request message. This message is sent to NSSAF instance interfacing with AAA-S or AAA-P if it is used.

The AAA-P, if present, relays the request to the NSSAAF.

2. The NSSAAF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE.

3. The NSSAAF request the relevant AMF to revoke the S-NSSAI authorization for the UE using the Nssaaf\_NSSAA\_RevocationNotification service operation.

The AMF is implicitly subscribed to receive Nssaaf\_NSSAA\_RevocationNotification service operations. The NSSAAF may discover the Callback URI for the Nssaaf\_NSSAA\_RevocationNotification service operation exposed by the AMF via the NRF. The AMF acknowledges the Notification of Revocation request.

4. The AMF sends the UE Configuration Update message to revoke the S-NSSAI from the current Allowed NSSAI, for any Access Type for which NSSAA had been successfully run on this S-NSSAI. The AMF provides a new Allowed NSSAI to the UE by removing the S-NSSAI for which authorization has been revoked. The AMF provides new rejected NSSAIs to the UE including the S-NSSAI for which authorization has been revoked. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and a Default NSSAI exists that requires no NSSAA or for which a NSSAA did not previously fail over this access, then the AMF may provide a new Allowed NSSAI to the UE containing the Default NSSAI. If no S-NSSAI is left in Allowed NSSAI for an access after the revocation, and no Default NSSAI can be provided to the UE in the Allowed NSSAI or a previous NSSAA failed for the Default NSSAI over this access, then the AMF shall execute the Network-initiated Deregistration procedure for the access as described in subclause 4.2.2.3.3 in TS 23.502 [8], and it shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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

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

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

DN Data Network

DNN Data Network Name

DU Distributed Unit

EAP Extensible Authentication Protocol

EDT Early Data Transmission

EMSK Extended Master Session Key

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

### \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*