**3GPP TSG-CT WG1 Meeting #131-eC1-21xxxx**

**Electronic meeting, 19 Aug – 27 Aug 2021**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3519** | **rev** | **1** | **Current version:** | **17.3.1** |  |
|  |
| *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:***  |  NSSAAF : Network slice-specific and SNPN authentication and authorization function  |
|  |  |
| ***Source to WG:*** | LG Electronics, Huawei, HiSilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-08-12 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe 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)Rel-17. (Release 17)* |
|  |  |
| ***Reason for change:*** |  In the SA2#145 e-meeting, S2-2105010 was agreed that the name of NSSAAF is changed to Network slice-specific and SNPN authentication and authorization function.It is needed to align with S2-2105010 to stage3 specification |
|  |  |
| ***Summary of change:*** |  NSSAAF term is changed from network slice specific authentication and authorization function to network slice specific and SNPN authentication and authorization function. |
|  |  |
| ***Consequences if not approved:*** | Misalignment with TS23.501 |
|  |  |
| ***Clauses affected:*** | 3.2, 5.4.7.1, 5.4.7.2.1, 5.4.7.2.2, 5.4.7.3.1 |
|  |  |
|  | **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:*** | Correction of cover page (CR number correction, Removal of linkage of SA2 spec, add Clauses affected)The use of actonym “NSSAAF” instead of full termination “Network Slice Specific and SNPN Authentication and Authorization Function (NSSAAF)” |

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

## 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].

4G-GUTI 4G-Globally Unique Temporary Identifier

5GCN 5G Core Network

5G-GUTI 5G-Globally Unique Temporary Identifier

5GMM 5GS Mobility Management

5G-RG 5G Residential Gateway

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

5GS 5G System

5GSM 5GS Session Management

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

5G-TMSI 5G Temporary Mobile Subscription Identifier

5QI 5G QoS Identifier

ACS Auto-Configuration Server

AKA Authentication and Key Agreement

AKMA Authentication and Key Management for Applications

A-KID AKMA Key Identifier

A-TID AKMA Temporary Identifier

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

APN Access Point Name

ATSSS Access Traffic Steering, Switching and Splitting

AUSF Authentication Server Function

CAG Closed access group

CHAP Challenge Handshake Authentication Protocol

DDX Downlink Data Expected

DL Downlink

DN Data Network

DNN Data Network Name

eDRX Extended DRX cycle

DS-TT Device-Side TSN Translator

EUI Extended Unique Identifier

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

ECIES Elliptic Curve Integrated Encryption Scheme

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

ESM EPS Session Management

FN-RG Fixed Network RG

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

Gbps Gigabits per second

GFBR Guaranteed Flow Bit Rate

GUAMI Globally Unique AMF Identifier

IAB Integrated access and backhaul

IMEI International Mobile station Equipment Identity

IMEISV International Mobile station Equipment Identity and Software Version number

IMSI International Mobile Subscriber Identity

IP-CAN IP-Connectivity Access Network

KSI Key Set Identifier

LADN Local Area Data Network

LCS LoCation Services

LMF Location Management Function

LPP LTE Positioning Protocol

MAC Message Authentication Code

MA PDU Multi-Access PDU

Mbps Megabits per second

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

N3IWF Non-3GPP Inter-Working Function

N5CW Non-5G-Capable over WLAN

N5GC Non-5G Capable

NAI Network Access Identifier

NITZ Network Identity and Time Zone

NR New Radio

ngKSI Key Set Identifier for Next Generation Radio Access Network

NPN Non-public network

NSSAA Network slice-specific authentication and authorization

NSSAAF Network Slice-Specific and SNPN authentication and authorization Function

NSSAI Network Slice Selection Assistance Information

OS Operating System

OS Id OS Identity

PAP Password Authentication Protocol

PCO Protocol Configuration Option

PEI Permanent Equipment Identifier

PNI-NPN Public Network Integrated Non-Public Network

PTI Procedure Transaction Identity

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

RACS Radio Capability Signalling Optimisation

(R)AN (Radio) Access Network

RFSP RAT Frequency Selection Priority

RG Residential Gateway

RPLMN Registered PLMN

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSNPN Registered SNPN

S-NSSAI Single NSSAI

SA Security Association

SDF Service Data Flow

SMF Session Management Function

SGC Service Gap Control

SNN Serving Network Name

SNPN Stand-alone Non-Public Network

SOR Steering of Roaming

SUCI Subscription Concealed Identifier

SUPI Subscription Permanent Identifier

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

Tbps Terabits per second

TNGF Trusted Non-3GPP Gateway Function

TSC Time Sensitive Communication

TWIF Trusted WLAN Interworking Function

TSN Time-Sensitive Networking

UDM Unified Data Management

UL Uplink

UPDS UE policy delivery service

UPF User Plane Function

UPSC UE Policy Section Code

UPSI UE Policy Section Identifier

URN Uniform Resource Name

URSP UE Route Selection Policy

V2X Vehicle-to-Everything

V2XP V2X policy

W-AGF Wireline Access Gateway Function

WLAN Wireless Local Area Network

WUS Wake-up signal

#### 5.4.7.1 General

The purpose of the network slice-specific authentication and authorization procedure is to enable the authentication, authorization and accounting server (AAA-S) via the Network Slice Specific and SNPN Authentication and Authorization Function (NSSAAF) to (re-)authenticate or (re-)authorize the upper layers of the UE.

The network slice-specific authentication and authorization procedure can be invoked for a UE supporting network slice-specific authentication and authorization procedure and for a HPLMN S-NSSAI (see subclause 5.15.10 in 3GPP TS 23.501 [8] and subclause 4.2.9.2 of 3GPP TS 23.502 [9]).

The network (re-)authenticates the UE using the EAP as specified in IETF RFC 3748 [34].

EAP has defined four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

The EAP-request message is transported from the network to the UE using the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message of the network slice-specific EAP message reliable transport procedure.

The EAP-response message to the EAP-request message is transported from the UE to the network using the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message of the network slice-specific EAP message reliable transport procedure.

If the (re-)authentication of the UE completes successfully or unsuccessfully, the EAP-success message or the EAP-failure message, respectively, is transported from the network to the UE using the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message of the network slice-specific result message transport procedure.

There can be several rounds of exchange of an EAP-request message and a related EAP-response message for the AAA-S via the NSSAAF to complete the (re-)authentication and (re-)authorization of the request for an S-NSSAI (see example in figure 5.4.7.1.1).

The AMF shall set the authenticator retransmission timer specified in subclause 4.3 of IETF RFC 3748 [34] to infinite value.

NOTE: The network slice-specific authentication and authorization procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer of the AMF do not occur.



Figure 5.4.7.1.1: Network slice-specific authentication and authorization procedure

##### 5.4.7.2.1 Network slice-specific EAP message reliable transport procedure initiation

In order to initiate the network slice-specific EAP message reliable transport procedure, the AMF shall create a NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message.

The AMF shall set the EAP message IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message to the EAP-request message which is generated by the AMF or provided by the AAA-S via the NSSAAF.

The AMF shall set the S-NSSAI IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message to the HPLMN S-NSSAI to which the EAP-request message is related.

The AMF shall send the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message and start timer T3575 per S-NSSAI (see example in figure 5.4.7.1.1).

Upon receipt of a NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message, the UE shall stop timer T3346 if running. The UE shall pass:

a) the EAP-request message received in the EAP message IE; and

b) the HPLMN S-NSSAI in the S-NSSAI IE;

to the upper layers. Apart from this action, the network slice-specific authentication and authorization procedure is transparent to the 5GMM layer of the UE.

##### 5.4.7.2.2 Network slice-specific EAP message reliable transport procedure accepted by the UE

When the upper layers provide an EAP-response message associated with the HPLMN S-NSSAI, the UE shall create a NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message.

The UE shall set the EAP message IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message to the EAP-response message.

The UE shall set the S-NSSAI IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message to the HPLMN S-NSSAI associated with the EAP-response message.

The UE shall send the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message. Apart from this action, the network slice-specific authentication and authorization procedure is transparent to the 5GMM layer of the UE.

Upon receipt of a NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message, the AMF shall stop timer T3575 and:

a) pass the EAP-responsemessage received in the EAP message IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message associated with the HPLMN S-NSSAI in the S-NSSAI IE to the upper layers; or

b) provide the EAP-response message received in the EAP message IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message associated with the HPLMN S-NSSAI in the S-NSSAI IE to the AAA-S via the NSSAAF.

##### 5.4.7.3.1 Network slice-specific EAP result message transport procedure initiation

In order to initiate the network slice-specific EAP result message transport procedure, the AMF shall create a NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message.

The AMF shall set the EAP message IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message to the EAP-success or EAP-failure message provided by the AAA-S via the NSSAAF.

The AMF shall set the S-NSSAI IE of the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message to the HPLMN S-NSSAI to which the EAP-success or EAP-failure message is related.

The AMF shall send the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message. The AMF shall retain the authentication result for the UE and the HPLMN S-NSSAI while the UE is registered to the PLMN (see subclause 5.15.10 in 3GPP TS 23.501 [8]).

Upon receipt of a NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message, the UE shall pass:

a) the EAP-success or EAP-failure message received in the EAP message IE; and

b) the HPLMN S-NSSAI in the S-NSSAI IE;

to the upper layers. Apart from this action, the network slice-specific authentication and authorization procedure is transparent to the 5GMM layer of the UE.