**3GPP TSG-CT WG1 Meeting #135-eC1-22xxxx**

**E-Meeting, 6th – 12th April 2022**

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

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | NSSAA performed for a UE operating in SNPN access operation mode | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-04-06 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | NSSAA can be performed for a UE operating in SNPN access operation mode. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | When NSSAA is performed for a UE operating in SNPN access operation mode, the S-NSSAI for which the NSSAA is performed is an SNPN S-NSSAI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Wrong S-NSSAI (HPLMN S-NSSAI) can be used for NSSAA in an SNPN. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 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:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

#### 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 or an SNPN S-NSSAI (see subclauses 5.15.10 and 5.30.2.9 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

\* \* \* Next Change \* \* \* \*

##### 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 or the SNPN 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 or the SNPN 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.

\* \* \* Next Change \* \* \* \*

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

\* \* \* Next Change \* \* \* \*

##### 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 or the SNPN 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 or the SNPN 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 or the SNPN 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.

\* \* \* End of Changes \* \* \* \*