**3GPP TSG-CT WG1 Meeting #129-eC1-212245**

**Electronic meeting, 19 April – 23 April 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | 3137 | **rev** | **1** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | SNN verification for SNPN supporting AAA-Server for primary authentication and authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | LG Electronics | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2021-04-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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-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:*** | | Based on the S2-2101081, the AUSF in SNPN may support primary authentication and authorization of UEs that use credentials from an AAA server in a Credential Holder (CH).  It means that if the UE supports access to an SNPN using credentials from a credential holders and there is no available/allowable SNPN which has own credential in the “list of subscriber data”, the UE can select another SNPN which uses credential of different SNPN and not in the “list of subscriber data”.  If the SNPN using credentials in CH is selected, the selected SNPN is not the SNPN having credential to be performed primary authentication. The SNPN to be performed primary authentictaion will be the SNPN in the “list of subscriber data”.  In current TS24.501, the UE shall check whether the network name field AT\_KDF\_INPUT attribute matches the SNPN identity saved in the UE in order to verify AT\_KDF. However, if the UE supports access to an SNPN using credential from CH, the UE stores many types of SNPN idendities.  - serving SNPN which does not have credential  - SNPN which has credential but not serving SNPN  - selected PLMN  In current specification, the UE checks whether the network name field of the AT\_KDF\_INPUT attribute matches the PLMN identity or the SNPN identity saved in the UE.  However, SNPN identity saved in the UE is ambiguous. Because, there are many types of SNPN identities. So, which SNPN identity is used should be clarified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is clarified which SNPN identity is used in order to verify SNN for supporting access to an SNPN using credentials from Credential Holders. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Due to invalid SNN verification, successful authentication can be misinterpreted as failure of authentication. As a results, it cause that normal UE can be considers as invalid UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.4.1.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Rev 1. Remove NOTE | | | | | | | | |

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

###### 5.4.1.2.2.2 Initiation

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40]. The AUSF shall set the AT\_KDF\_INPUT attribute of the EAP-request/AKA'-challenge message to the SNN. The SNN is in format described in subclause 9.12.1. The AUSF may include AT\_RESULT\_IND attribute in the EAP-request/AKA'-challenge message.

The network shall select an ngKSI value. If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall select a different ngKSI value. The network shall send the selected ngKSI value to the UE along with each EAP message. The network shall send the ABBA value as described in subclause 9.11.3.10 to the UE along with the EAP request message and EAP-success message.

Upon receiving an EAP-request/AKA'-challenge message, the UE shall check whether the UE has a USIM, shall check the key derivation function indicated in AT\_KDF attributes as specified in IETF RFC 5448 [40], and if the value of the Key derivation function field within the received AT\_KDF attribute, is of value 1, shall check:

a) whether the network name field of the AT\_KDF\_INPUT attribute is the SNN constructed according to subclause 9.12.1; and

b) whether the network name field of the AT\_KDF\_INPUT attribute matches the PLMN identity or the SNPN identity of the selected SNPN saved in the UE.

When not operating in SNPN access operation mode, the PLMN identity the UE uses for the above network name check is as follows:

a) when the UE moves from 5GMM-IDLE mode to 5GMM-CONNECTED mode, until the first handover, the UE shall use the PLMN identity of the selected PLMN; and

b) after handover or inter-system change to N1 mode in 5GMM-CONNECTED mode:

1) if the target cell is not a shared network cell, the UE shall use the PLMN identity received as part of the broadcast system information;

2) if the target cell is a shared network cell and the UE has a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the 5G-GUTI; and

3) if the target cell is a shared network cell and the UE has a valid 4G-GUTI, but not a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the 4G-GUTI.

When operating in SNPN access operation mode, the SNPN identity the UE uses for the above network name check is the SNPN identity of the selected SNPN.

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