**3GPP TSG-SA3 Meeting #105-e  *draft\_S3-213977-r1***

e-meeting, 08 - 19 November 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1209** | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Rel-17 security aspects on MINT feature | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | LG Electronics | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2021-11-01 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | There is an open question in TS 23.501 clause 5.40.4 on Disaster Roaming service indication from AMF to other NFs (e.g., AUSF and UDM) for the MINT feature.  As this issue is related to the authentication and subscription information checking procedure, it is required to capture the aspect in SA3 specification as well.  There are two options on the table provided by SA2 to indicate a Disaster Condition to AUSF/UDM.   1. "Disaster Roaming service indication" is transferred from AMF to AUSF/UDM 2. No additional signaling. The Disaster Condition is notified to AUSF/UDM via OAM based on the operator policy or the request by the government agencies when a disaster roaming occurs.   It is proposed to support both options for operator's flexible deployment and preference.  This CR is trying to trigger the discussion in SA3 on the security aspect of MINT feature as identified by SA2. The content of this CR can be updated or even partly removed upon the consensus on the selection of options. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to update the initiation of authentication procedure to accommodate the MINT feature and also update the corresponding services provided by AUSF and UDM. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The authentication of UE and subscription information checking when a Disaster Condition occurs cannot be performed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2, 14.1.2, 14.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

### 6.1.2 Initiation of authentication and selection of authentication method

The initiation of the primary authentication is shown in Figure 6.1.2-1.



Figure 6.1.2-1: Initiation of authentication procedure and selection of authentication method

The SEAF may initiate an authentication with the UE during any procedure establishing a signalling connection with the UE, according to the SEAF's policy. The UE shall use SUCI or 5G-GUTI in the Registration Request.

The SEAF shall invoke the Nausf\_UEAuthentication service by sending a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF whenever the SEAF wishes to initiate an authentication.

The Nausf\_UEAuthentication\_Authenticate Request message shall contain either:

- SUCI, as defined in the current specification, or

- SUPI, as defined in TS 23.501 [2].

The SEAF shall include the SUPI in the Nausf\_UEAuthentication\_Authenticate Request message in case the SEAF has a valid 5G-GUTI and re-authenticates the UE. Otherwise the SUCI is included in Nausf\_UEAuthentication\_Authenticate Request. SUPI/SUCI structure is part of stage 3 protocol design.

The Nausf\_UEAuthentication\_Authenticate Request shall furthermore contain:

- the serving network name, as defined in sub-clause 6.1.1.4 of the present document.

NOTE 2: The local policy for the selection of the authentication method does not need to be on a per-UE basis, but can be the same for all UEs.

The Nausf\_UEAuthentication\_Authenticate Request may furthermore contain:

- Disaster Roaming service indication, as specified in TS 23.502[8] clause 4.2.2.2

Upon receiving the Nausf\_UEAuthentication\_Authenticate Request message, the AUSF shall check that the requesting SEAF in the serving network is entitled to use the serving network name in the Nausf\_UEAuthentication\_Authenticate Request by comparing the serving network name with the expected serving network name. The AUSF shall store the received serving network name temporarily. If the serving network is not authorized to use the serving network name, the AUSF shall respond with "serving network not authorized" in the Nausf\_UEAuthentication\_Authenticate Response.

NOTE 1: The AUSF and the UDM may be configured with Disaster Condition via OAM based on operator policy and the request by the government agencies.

For the Disaster Roaming, the AUSF shall check the local configuration based on SUCI or SUPI and the serving network name. Based on the local configuration, the AUSF sends Nudm\_UEAuthentication\_Get Request to the UDM.

The Nudm\_UEAuthentication\_Get Request sent from AUSF to UDM includes the following information:

- SUCI or SUPI;

- the serving network name;

- if received from SEAF, Disaster Roaming service indication;

Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

Based on SUPI, the UDM/ARPF shall choose the authentication method.

NOTE 3: The Nudm\_UEAuthentication\_Get Response in reply to the Nudm\_UEAuthentication\_Get Request and the Nausf\_UEAuthentication\_Authenticate Response message in reply to the Nausf\_UEAuthentication\_Authenticate Request message are described as part of the authentication procedures in clause 6.1.3.

For the Disaster Roaming, the UDM shall check the local configuration based on SUCI or SUPI and the serving network name. Based on the local configuration, the UDM proceeds with an applicable authentication method.

\*\*\* 2nd CHANGE \*\*\*

### 14.1.2 Nausf\_UEAuthentication service

**Service operation name:** Nausf\_UEAuthentication\_authenticate.

**Description:** Authenticate the UE and provides related keying material.

**Input, Required:** One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.

2. In the subsequent authentication requests depending on the authentication method:

a. 5G AKA: Authentication confirmation message with RES\* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS).

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

**Input, Optional:** Disaster Roaming service indication.

**Output, Required:** One of the options below.

1. Depending on the authentication method:

a. 5G AKA: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.

b. EAP-AKA’: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

**Output, Optional:** SUPI if the authentication was initiated with SUCI.

\*\*\* 3rd CHANGE \*\*\*

### 14.2.2 Nudm\_UEAuthentication\_Get service operation

**Service operation name:** Nudm\_UEAuthentication\_Get

**Description:** Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

**Inputs, Required:** SUPI or SUCI, serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS), Disaster Roaming service indication.

**Outputs, Required:** Authentication method

Outputs, Optional**:** SUPI if SUCI was used as input. Depending on the authentication method, authentication data (e.g. AKA authentication vector) for the SUPI. AKMA Indication and Routing indicator, if the subscriber has an AKMA subscription (see TS 33.535 [91]).

\*\*\* END OF CHANGES \*\*\*