**3GPP TSG-SA3 Meeting #107-eS3-220964**

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **TS 33.256** | **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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Resolving of EN in Clause 5.2.1.4 UUAA re-authentication procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo, Huawei Hisilicon, Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | ID\_UAS | | | | |  | ***Date:*** | | | 2022-05-02 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | In TS 33.256 Clause ‘5.2.1.4 UUAA re-authentication procedure (5G)’, there is an EN as follows:  Editor's Note: For USS initiated re-authentication, how the USS/UTM contacts the right UAS NF which stores the UUAA context corresponding to an UAV is FFS  The related clarification has already been agreed for EPS, but it is missed to be added for 5GS.  Merger of S3-220980, S3-220804, and S3-220964 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarifications are added to address the EN on contacting the right UAS NF for UUAA re-authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | If no clarification is added to address the above EN, then the specification will be incomplete and for the 5GS case the USS cannot reach the right UAS NF to initiate the UUAA re-authentication when required. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.1.4, 5.2.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Merger of S3-220980, S3-220804, and S3-220964 | | | | | | | | |

\*\*\* Start of Change 1 \*\*\*

#### 5.2.1.4 UUAA re-authentication procedure (5G)

As described in clause 5.2.1.1, the USS or the AMF (if support UUAA during registration) may initiate the Re-authentication procedure for the UAV at any time.

This clause describes the USS initiated Re-authentication procedure (the AMF initiated Re-authentication procedure is described in the clause 5.2.1.2). The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).



Figure 5.2.1.4-1: UUAA re-authentication in 5GS

1. The USS sends a re-authentication request for the UAV to UAS-NF that includes GPSI, CAA-Level UAV ID, and an authentication message. It may contain the PDU Session IP address if available. The USS shall use the UAS NF Routing information received during the previous successful UUAA related to GPSI for sending the re-authentication request.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UAA. The UAS-NF verifies the USS re-authentication request by checking whether the GPSI and the USS identifier match of the USS requesting the re-authentication the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the re-authentication procedures if match.

NOTE 1: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

The UAS NF determines whether the target NF is an AMF or an SMF.

- If the target NF is an AMF, the UAS NF further determines the target AMF for re-authentication and continues step 3a.

- If the target NF is an SMF, the UAS NF further determines the target SMF for re-authentication and continues step 3b.

3a or 3b. The UAS NF sends to either the target AMF or the target SMF the UAA re-authentication request for the UE identified by the GPSI and for the SMF only the PDU Session IP address if available.

4. The UAS NF responses the USS that the UAA Re-authentication has been initiated.

5a. If the target NF is an AMF, the AMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.2 (step 2 to step 9).

5b. If the target NF is an SMF, the SMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.3 (step 2 to step 7).

\*\*\* End of Change 1 \*\*\*

\*\*\* Start of Change 2 \*\*\*

#### 5.2.2.3 UUAA re-authentication procedure (EPC)

The USS the Re-authentication procedure for the UAV at any time. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).



Figure 5.2.2.3-1: UUAA re-authentication in EPS

1. The USS sends a re-authentication request for the UAV to UAS-NF that includes GPSI, CAA-Level UAV ID, and an Authentication message. It may contain the PDU Session IP address if available. The USS shall use the UAS NF Routing information received during the previous successful UUAA related to GPSI for sending the re-authentication request.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UAA. The UAS-NF verifies the USS re-authentication request by checking whether the GPSI and the USS identifier of the USS requesting the re-authentication match the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the re-authentication procedures if match.

NOTE 1: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

3. The UAS NF sends to the target SMF+PGW-C the UAA re-authentication request for the UE identified by the GPSI.

4. The UAS NF responses the USS that the UAA Re-authentication has been initiated.

5. The SMF+PGW-C initiates re-authentication of the UAV as UUAA described in the clause 5.2.2.2 (step 4c to step 7).

\*\*\* End of Change 2 \*\*\*