**3GPP TSG-SA3 Meeting #115 *draft S3-2401003-r1 merges 431 in S3-240768***

Athens, Greece, 26th February - 1st March 2024

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **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 |  |

|  |
| --- |
|  |
| ***Title:***  | Cleans up AMF and SMF relation for UUAA |
|  |  |
| ***Source to WG:*** | Lenovo, Huawei |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2024-02-19 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Alignment to approved SP-231244 on Cleanup of UUAA-MM and UUAA-SM relation. SA2 (See TS 23.256 V18.1.0) wants to execute the UUAA repeatedly during PDU session establishment irrespective of any recent successful UUAA results available from the UE registration phase. |
|  |  |
| ***Summary of change:*** | Cleaned UUAA-MM and UUAA-SM relation. |
|  |  |
| ***Consequences if not approved:*** | UUAA may be skiped during PDU session establishment if already a successful UUAA performed at registration |
|  |  |
| ***Clauses affected:*** | 5.2.1.1, 5.2.1.3 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*Start of change 1\*\*\*\*\*

#### 5.2.1.1 General

The UAV USS authentication and authorization (UUAA) is the procedure to ensure that the UAV can be authenticated and authorized by a USS before the connectivity for UAS services is enabled. This clause specifies the relationship between primary authentication (as described in clause 6.1 in TS 33.501 [2]) and UUAA. An UAV is allowed to perform UUAA with the USS/UTM only after the UAV (UE) has completed successfully primary authentication.

It may be triggered by the AMF when UAV is registering with 5GS or triggered by the SMF during the PDU session establishment procedure. The UUAA procedure may also be triggered by a USS for re-authentication if the USS had authenticated the UAV. Network support for UUAA during registration is optional while it is mandatory during the PDU Session establishment. UE Support for UUAA during registration and during the PDU Session establishment is mandatory.

The AMF or SMF triggers the UUAA procedure if the UAV has an Aerial UE subscription and the UAV requests access to UAS services by providing the CAA-Level UAV ID of the UAV in the Registration Request or PDU Session Establishment Request.

The UUAA is performed between the UAV and the USS. The UAV is authenticated based on the CAA-Level UAV ID and credentials associated to the CAA-Level UAV ID. The authentication messages are included in a transparent container and conveyed between the UAV and the USS via a 3GPP UAS NF.

NOTE: The provision of CAA-Level UAV ID, credentials, and the actual authentication methods and information that needs to be sent to perform the UUAA are out of scope of the 3GPP specifications.

On successful completion of a UUAA, the USS can send UAS security information in the UUAA Authorization Payload to the UAV. The contents of that security information are out of scope of the 3GPP specifications.

The UUAA procedure at registration in 5G is described in the clause 5.2.1.2 and the UUAA procedure during PDU session establishment procedure is described in the clause 5.2.1.3.

At any time after the initial registration, the USS or the AMF (when the networking supports UUAA during registration) may initiate the Re-authentication procedure for the UAV. The AMF initiated Re-authentication procedure is described in the clause 5.2.1.2, whereas the USS initiated Re-authentication procedure is described in the clause 5.1.2.4.

Figure 5.2.1.1-1 provides an example of how UUAA fits into the 5GS procedures. The complete description of this flow is given in TS 23.256 [3].



Figure 5.2.1.1-1: UUAA in 5GS

1. The UE sends a Registration Request message to the AMF. The UE may provide a CAA-Level UAV ID, and optionally a USS address/IP address, to indicate the request is registering for UAS services. In case the CAA-Level UAV ID and/or USS address/IP address is configured not to be sent in plain text, e.g., the USS address or an IP address not to be exposed in public, the CAA-Level UAV ID, and USS/IP address if available, shall be sent after the NAS security is established.

2. AMF completes security set up including primary authentication as needed.

3. After successful Primary authentication, AMF determines whether UUAA is required for the UE. UUAA shall only be triggered if the UE has provided a CAA-Level UAV ID and has a valid Aerial UE subscription. AMF may skip UUAA if the UE has completed UUAA successfully before and the UE UUAA is current, i.e., the UE's authentication and authorization has not been revoked after a previous successful UUAA.

4a. AMF shall return a Registration Accept message to the UE and indicate that UUAA is pending.

4b. UE may send a Registration Complete message to acknowledge the AMF.

5. AMF triggers the UUAA procedure if determined needed in step 3 as described in clause 5.2.1.2.

The following procedure is for UUAA during PDU session establishment:

6. The UE sends a PDU Session Establishment Request message to the SMF including a CAA-Level UAV ID to indicate the request is for UAS services.

7. The SMF determines whether UUAA is required for the UE. UUAA shall only be triggered if the UE has provided a CAA-Level UAV ID and has a valid Aerial UE subscription. SMF may skip UUAA, if the UE has completed UUAA successfully with the same USS/DN before, i.e., in previous PDU Session Establishment procedures and a successful UUAA result is available.

8. The SMF triggers the UUAA procedure if determined needed at step 7 as described in clause 5.2.1.3.

\*\*\*\*\*End of change 1\*\*\*\*\*

\*\*\*\*\*Start of change 2\*\*\*\*\*

#### 5.2.1.3 UUAA Procedure during PDU Session Establishment

The SMF may trigger a UUAA procedure during the PDU session establishment procedure with details described below, which considers only the security related (see TS 23.256 [3] for full details of the flows).



Figure 5.2.1.3-1: UUAA Procedure at PDU Session Establishment

1. The SMF determines whether UUAA is required as described in the clause 5.2.1.1 if the UE provides a CAA-Level UAV ID indicating UAS services and optionally the Aviation Payload if provided by the UE for USS to authenticate the UAV in the PDU Session Establishment request. The SMF triggers a UUAA procedure after the determination in step 7 in the clause 5.2.1.1.

2. The SMF sends a message Nnef\_Auth\_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container if provided by the UE. The SMF may include other information in the request as in TS 23.256 [3].

3. The UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address. Only authorized USS shall be used in order to ensure only legitimate entities can provide authorization for UAVs. The UAS NF sends an Authentication Request to the USS which includes the GPSI, the CAA-Level UAV ID, the UAS NF Routing information (e.g., a FQDN or IP address) which uniquely identifies the NF located in the 3GPP network that handles the UAV related messages exchanges with the corresponding external USS/UTM, and the transparent container. Other information may also be included in this message (see TS 23.256 [3]).

4. The USS and the UE exchange multiple Authentication messages:

NOTE 1: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by the USS. The method used to authenticate the UE (e.g. whether over EAP or not) and the content of Authentication Messages (e.g. EAP packets) to support that method are out of scope of 3GPP. The USS determines the authentication method used.

4a. The USS replies to UAS NF with the Authentication Response message. It shall include the GPSI, a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container to the SMF.

4c. The SMF forwards the transparent container to the AMF, which then forwards to the UE over a NAS MM transport message.

4d. The UE responses the AMF with an Authentication message embedded in a transparent container over a NAS MM transport message. The AMF forwards to the SMF.

4e. The SMF sends a message Nnef\_Auth\_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container provided by the UE.

4f. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID and the transparent container.

NOTE 2: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by USS. The method used to authenticate the UE and the content of Authentication Messages are out of scope of 3GPP.

5. The USS sends the UAS NF an Authentication Response message. The Authentication Response shall include the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and a UUAA Authorization Payload that contains UAS security information if the USS has such information to send to the UAV.

NOTE 3: The content of security information (e.g., key material to help establish security between UAV and USS/UTM) is not in 3GPP scope.

If UUAA successful, the UAS NF stores the UAV UEs' UUAA context, including the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

NOTE 4: The USS Identifier is used to ensure that a USS requesting a subsequent re-authentication or revocation is the same one that authenticated the UAV in the first place. The USS identifier is based on the security link on the interface between UAS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate, prior to the UUAA procedures).

6. The UAS NF sends the SMF an Authentication Response message, including the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and the UUAA Authorization Payload received in step 5.

The SMF stores the results, together with the GPSI and the CAA-level UAV ID.

7. The SMF sends the UUAA result (success/failure), and the UUAA Authorization Payload received in step 5 to the UE. The message(s) used in step 7 and any further actions the UE and SMF take are given in TS 23.256 [3].

8. The UE on receiving the UUAA result as success, shall store the authorization information if received such as, CAA-level UAV ID, and UAS Security information.

\*\*\*\*\*End of change 2\*\*\*\*\*