**3GPP TSG-SA3 Meeting #108e *S3-221747***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2022-08-10 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | This contribution proposes to remove ENs related to CAA level UAV ID sent to UE. When a UE is associated with two or more UAV IDs, which is possible in Rel-17, it is necessary to include CAA-Level UAV ID to avoid ambiguity. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Removed 5 similar ENs related to CAA level ID (no normative text change) in the clauses 5.2.1.2, 5.2.1.3, 5.2.1.5, 5.2.2.2, 5.2.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The specification is not completed | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.1.2, 5.2.1.3, 5.2.1.5, 5.2.2.2, 5.2.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.2.1.2 UUAA Procedure at Registration

The UUAA procedure at registration is triggered by an AMF with the details described below, which considers only the security related parameters (see TS 23.256 [3] for full details of the flows). For an AMF initiated re-authentication, the procedure starts from the step 2.



Figure 5.2.1.2-1: UUAA Procedure at Registration

1. The AMF triggers the UUAA procedure as described in clause 5.2.1.1.

2. The AMF sends a message Nnef\_Auth\_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the Aviation Payload if provided by the UE for USS to authenticate the UAV. The AMF 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. The Authentication Request shall include the GPSI, the CAA-Level UAV ID, a UAS NF Routing information (e.g., an FQDN or IP address) which uniquely identifies the UAS 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 as in TS 23.256 [3].

4. The USS and the UE exchange 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 and a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container received in 4a to the AMF with the GPSI.

4c. The AMF forwards the transparent container to the UE over NAS MM transport messages.

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

4e. The AMF 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.

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.

NOTE 2: The content of security information (e.g. key material to help establish security between UAV and USS/UTM) is not in 3GPP scope.

The UAS NF stores the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

NOTE 3: 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 USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

6. The UAS NF sends the AMF 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.

7. The AMF sends to the UE the UUAA result (success/failure) received in step 6. The message(s) used in step 7 are given in TS 23.256 [3].

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

8. If UUAA result is success, the AMF sends to the UE the UUAA Authorization Payload, received in step 6, during a UCU procedure as described in TS 23.256 [3]. The UE shall store the authorization information if received such as UAS Security information along with the CAA-level UAV ID.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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 and if the UUAA result is not received from the AMF, 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 USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

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 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.2.2.2 UUAA procedure

The UUAA procedure is triggered by an SMF+PGW-C with the details described below, which considers only the security related parameters (see TS 23.256 [3] for full details of the flows).



Figure 5.2.2.2-1: UUAA procedure

2. The SMF+PGW-C sends a message Nnef\_Auth\_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the Aviation Payload if provided by the UE for USS to authenticate the UAV. The SMF+PGW-C 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. The Authentication Request shall include the GPSI, the CAA-Level UAV ID, a UAS NF Routing information (e.g., a FQDN or IP address) which uniquely identifies the UAS 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 as in TS 23.256 [3].

4. The USS and the UE exchange 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 and a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container received in 4a to the SMF+PGW-C with the GPSI.

4c. The SMF+PGW-C forwards the transparent container to the UE over NAS MM transport messages.

4d. The UE response to the SMF+PGW-C with an Authentication message embedded in a transparent container over a NAS MM transport message.

NOTE 2: The method of transporting messages between the SMF+PGW-C and UE is described in TS 23.256 [3].

4e. The SMF+PGW-C 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.

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.

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.

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 USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

The UAS NF stores the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

6. The UAS NF sends the SMF+PGW-C 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.

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

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

8. If UUAA result is success, the UE shall store the authorization information if received such as UAS Security information along with the CAA-level UAV ID.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*