**3GPP TSG-SA2 Meeting #147-e *S2-2107151r04***

**Online, Elbonia, 18th Oct 2021 - 22nd Oct 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.256** | **CR** | **0003** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarifications for UUAA-SM procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | LG Electronics | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | ID\_UAS | | | | |  | ***Date:*** | | | 2021-10-07 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | TS 23.256 does not specify clearly how to handle PDU session during UUAA-SM procedure when UUAA failure.  TS 23.256 specifies about an indication that “indication whether the UAS service releated network resource can be released in case of UUAA failure” to solve the problem that removing all PDU sessions for a UAV because of UUAA re-authentication failure may lead to loss of command and control and the ability to tracking the UAV. TS 23.256 specifies that this indication is used for UUAA-MM re-authentication failure. But there is the same problem when UUAA-SM re-authentication failure case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarification that if UUAA-SM failed during PDU session establishment, SMF will reject the PDU session establishment.  It is proposed to use “Indication whether the UAS service related network resource can be released in case of UUAA failure” for UUAA-SM re-authentication failure case.  Removing a duplicated sentence in NOTE 1. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | It is not clear how to handle PDU session during UUAA-SM procedure when UUAA failure.  Removing all PDU sessions for a UAV because of UUAA re-authentication failure may lead to loss of command and control and the ability to tracking the UAV | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | |  | | |
| ***affected:*** | |  | **X** | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

#### 5.2.3.2 USS UAV Authorization/Authentication (UUAA) during the PDU Session Establishment

The USS UAV Authorization/Authentication (UUAA) is triggered by the SMF during the PDU Session Establishment, specified in TS 23.502 [3], clause 4.3.2.2 and additionally based on the SM subscription data obtained from UDM, and the Service Level Device Identity provided by the UE in the PDU Session establishment request.



Figure 5.2.3.2 -1: UUAA during PDU Session Establishment

The procedure assumes that the UE/UAV has already registered on the AMF.

0. Steps 1 - 5 as in TS 23.502 [3] figure 4.3.2.2.1-1.

The SMF determines that it needs to invoke UAS NF/NEF service operation for UUAA Authentication/Authorization of the PDU session establishment request based on the provided DNN/S-NSSAI.

The UAV includes the Service Level Device Identity (e.g. the CAA-Level UAV ID of the UVA) and may include the Authentication Server Address (i.e. the USS address) and optionally Authentication Data (i.e. the UUAA Aviation Payload) in the PDU Session Establishment request.

The SMF identifies the UAS NF/NEF based on local configuration or using UE provided identity e.g. USS address.

1. The SMF invokes Nnef\_Authentication\_Authenticate service operation, including the Service Level Device Identity (that contains the CAA-Level UAV ID of the UAV), DNN, S-NSSAI, and may include the Authentication Server Address (i.e. the USS address) and the Authentication Data (i.e. the UUAA Aviation Payload) if it was provided by the UE, GPSI, optionally UAV location, PEI if available, and the UE IP Address if available. The UAV location is the User Location Information provided by the AMF (e.g. Cell ID). The UAS NF/NEF selects a USS based on either the Service Level Device Identity (i.e. CAA-Level UAV ID of the UAV) or the Authentication Server address (i.e. USS address) as described in clause 4.4.2.

If a UUAA has been performed at Registration there is no need for the USS to perform UUAA at PDU Session establishment and steps 1 to 5 is not performed.

2. From UAS NF/NEF to USS: Naf\_Authentication\_Authenticate\_service operation forwarding the authentication request received information from the SMF. UAS NF may translate the Cell ID received as part of UAV location in the Nnef\_Authentication\_Authenticate request at step 1 into a corresponding geographic area and/or may further obtain the UE location information using Location Service Procedures as defined in TS 23.273 [8] and include them in the Naf\_Authentication\_Authenticate message towards the USS e.g. to support geo-caging functionality.

3. [Conditional] Multiple round-trip messages as required by the authentication method used by USS. N33\_Authentication\_Authenticate response messages from USS shall include GPSI and may include a authentication message based on authentication method used that is forwarded transparently to UE over NAS MM transport messages. The authentication message in step3e may contain UUAA Aviation Payload required by the USS if it was not provided by the UE before.

4. From USS to UAS NF/NEF: Naf\_Authentication\_Authenticate response.

The USS sends Naf\_Authentication\_Authenticate response to the UAS NF/NEF with the Authentication/Authorization result containing the UUAA result and indication whether the UAS service related network resource can be released in case of UUAA failure for re-authentication or re-authorization, optionally a Service Level Device Identity containing the new CAA-Level UAV ID, requested policy information, an Authorization Data (i.e. the UUAA Authorization Payload). The requested policy information from USS may contain a DN Authorization Profile Index and/or a DN authorized Session AMBR.

NOTE 1: The USS stores a mapping between CAA-Level UAV ID and the External Identifier (i.e. GPSI as defined in clause 4.5.3). The External Identifier (GPSI) and/or UAV IP Address can be used at a later point by the USS for accessing various services exposed by 3GPP network e.g. location information retrieval, monitoring event configuration, requesting dedicated policies for e.g. C2, etc.

5. The UAS NF/NEF confirms the successful Authentication/Authorization of the PDU Session. The UAS NF/NEF stores the UUAA result together with the GPSI. UAS NF/NEF forwards the Authentication/Authorization result, a Service Level Device Identity containing the new CAA-Level UAV ID, if received from the USS, and the Authorization Data (i.e. the UUAA Authorization Payload), if received from the USS, to the SMF. If the authentication/authorization is successful, the SMF shall subscribe for notifications from UAS NF/NEF which may be used to trigger re-authentication, update authorization data or revoke authorization of the UAV, upon receipt of such request from the USS.

6. [Conditional] If the authentication/authorization is successful, the USS shall subscribe to the PDU Session Status Event as described in steps 1-5 in Figure 4.15.3.2.3-1 of TS 23.502 [3]. This step can be executed in parallel to step 4. The UAS NF/NEF shall use the DNN, S-NSSAI received from the SMF in step 1 to subscribe to the PDU Session Status Event notification.

7. The PDU Session establishment continues with steps 7 to 21 in Figure 4.3.2.2.1-1of TS 23.502 [3] and completes. In the step 7b in Figure 4.3.2.2.1-1of TS 23.502 [3], if the SMF receives the DN Authorization Profile Index from the UAS NF/NEF, it sends the DN Authorization Profile Index to retrieve the PDU Session related policy information (described in clause 6.4 of TS 23.503 [9]) and the PCC rule(s) (described in clause 6.3 of TS 23.503 [9]) from the PCF. If the SMF receives the DN authorized Session AMBR in from the UAS NF/NEF, it sends the DN authorized Session AMBR within the Session AMBR to the PCF to retrieve the authorized Session AMBR (described in clause 6.4 of TS 23.503 [9]).

The SMF transfers the Authentication/Authorization result, the Service Level Device Identity containing the new CAA-Level UAV ID and the Authorization Data (i.e. the UUAA Authorization Payload) to the UAV as in steps 11, 12 and 13 in figure 4.3.2.2.1-1 of TS 23.502 [3].

If the authentication/authorization result is a failure, the SMF rejects the PDU session establishment with a cause indicating that authentication/authorization failed.

8. [Conditional] If the USS in step 6 subscribed to the PDU Session Status Event the SMF will, as described in steps 6-7 in Figure 4.15.3.2.3-1 of TS 23.502 [3], detect when the PDU Session is established, and send the PDU Session Establishment event report to the UAS NF/NEF by means of Nsmf\_EventExposure\_Notify message, including GPSI and the UE IP Address. Then, the UAS-NF/NEF forwards the event message to the USS.

If UUAA-SM fails during a Re-authentication and Re-authorization and the USS has indicated that the network resources can be released, SMF may trigger PDU Session release for UAS services with a cause indicating that authentication/authorization failed.

NOTE 2: If C2 information reference is available from USS during the initial PDU Session Establishment procedure the SMF can interact with the PCF to set up a predefined PCC rule(s) profile for the C2 communication.

\* \* \* \* End of Changes \* \* \* \*