**3GPP TSG-SA3 Meeting #107-e *S3-220986r1***

**e-meeting, 16 - 20 May 2022** *revision of S3-220986*

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.256** | **CR** | **0015** | **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 | **x** | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Resolving the ENs on protection of UAS data |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | ID\_UAS |  | ***Date:*** | 2022-05-03 |
|  |  |  |  |  |
| ***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:*** | There are several ENs on the protection of UAS data. This is the responsibility of the USS/UAV provider and these should ensure that this data is protected independently of any protection provided by the 3GPP network as this ensures that data is protected in all cases, e.g. there is no guarantee that this data is sent over a 3GPP network.  |
|  |  |
| ***Summary of change:*** | Remove the ENs  |
|  |  |
| ***Consequences if not approved:*** | Specification still contains ENs.  |
|  |  |
| ***Clauses affected:*** | 5.1, 5.2.2.2, 5.4.2, 5.4.3 |
|  |  |
|  | **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:*** | Rev1 add note in clause 5.1 |

**\*\*\*\* START OF CHANGES \*\*\*\***

5.1 General

Clause 5 contains the security details for the various UAS features that are given in TS 23.256 [3].

NOTE: Protection of UAS traffic is the responsibility of the USS/UAV provider and these should ensure that this data is protected independently of any protection provided by the 3GPP network as this ensures that data is protected in all cases.

**\*\*\*\* NEXT CHANGE \*\*\*\***

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**

1. The SMF+PGW-C decides to trigger the UUAA procedure as described in TS 33.256 [3].

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.

Editor's Note: It is FFS whether the inclusion of CAA level ID in step 6 and its storage at step 7 align with TS 23.256. As they were added for alignment purposes only, no action on this functionality is needed in stage 3 until this EN is resolved.

**\*\*\*\* NEXT CHANGE \*\*\*\***

5.4.2 UAV pairing Authorization with UAVC in 5GS

Pairing authorization may be performed during a PDU Session Establishment/PDU Session Modification after a successful UAA between the UAV and the USS/UTM. If no successful UUAA has been performed, then the pairing authorization can occur during the UUAA-SM procedure (see clause 5.2.5.2.1 of TS 23.256 [3] for full details). This procedure follows the clause 5.2.1.3 with the following additions:

- the UE provides pairing information (if available) in a C2 authorization payload in the PDU Session Establishment message and this is forwarded to the USS in steps 2 and 3; and

- after a successful authentication and before sending the message in step 5, the USS performs C2 authorization considering the included pairing information, the CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result) if the USS has such information to send. This is passed to the UE in steps 5-7. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope.

UAV pairing authorization during the PDU Session Establishment/PDU Session Modification procedure is described as follows. Full details of the procedures are given in TS 23.256 [3].

****

**Figure 5.4.2-1: UAV pairing authorization during PDU Session Establishment**

1. When the UAV needs a new dedicated PDU session for connectivity to the UAV-C, the UE initiates a PDU Session Establishment procedure. When the UE wants to use an existing PDU session for connectivity to the UAV-C, the UE initiates a PDU Session Modification procedure. The UE shall include the following IEs in the PDU session establishment/modification request: a CAA-Level UAV ID, a DNN/S-NSSAI implying dedicated connectivity to UAV-C, and UAV pairing information, which includes any needed authorization information, if available.

The pairing information includes the CAA-level UAV IDs of the requesting UAV and identification information of UAV-C to pair. The USS may also use its locally configured pairing information for UAV and UAV-C pairing authorization which takes precedence over UAV provided pairing information.

NOTE: The integrity protection of pairing information is recommended. It is performed by the USS, and is not in scope of 3GPP system.

2. The SMF determines whether the UAV pairing authorization is required based on UAV's aerial subscription, presence of CAA-Level UAV ID, and DNN/S-NSSAI indicating the UAV service, as step 7 in clause 5.2.1.1:

 The SMF invokes the authorization procedure with the USS via UAS-NF. The USS will perform C2 authorization taking account of the included pairing information, which includes any needed authorization information, if available, the CAA-Level UAV ID, and GPSI, etc.

 The USS informs the SMF via the UAS NF of the authorization results. The authorization information includes the IP address of the UAV-C and a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result) if the USS has such information to send. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope. The other information contained in this message is given in TS 23.256 [3].

3. The SMF informs the UE the paring authorization result in the PDU Session Establishment Accept message/PDU session Modification Command, which may include a new CAA-level UAV ID. The UE shall store the Pairing authorization result and authorization information.

The PDU Session Establishment/Modification continues and completes as described in TS 23.256 [3].

The UAV pairing authorization can be revoked by the USS at any time.

Besides, the paired UAV-C can be replaced by a new UAV-C by the USS at any time.

5.4.3 UAV pairing Authorization with UAVC in EPS

Pairing authorization may be performed during a PDN Connection Establishment/PDN Connection Modification procedure after a successful UUAA between the UAV and the USS/UTM. If no successful UUAA has been performed, then the pairing authorization can occur during the during the UUAA procedure (see clause 5.2.5.3.0 of TS 23.256 [3] for full details). This procedure follows the clause 5.2.2.2 with the following additions:

- the UE provides pairing information (if available) in a C2 authorization payload and this is forwarded to the USS in steps 2 and 3; and

- after a successful authentication and before sending the message in step 5, the USS performs C2 authorization considering the included pairing information, the CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result, i.e., whether the UAV is allowed to be paired with the UAV-C) if the USS has such information to send. This is passed to the UE in steps 5-7. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope.

UAV pairing authorization during the PDN Connection Establishment/ Modification procedure is described as follows. Full details of the procedures are given in TS 23.256 [3].

****

**Figure 5.4.3-1: UAV pairing authorization during PDN Connection Establishment/Modification**

1. When the UAV needs a new dedicated PDU session for connectivity to the UAV-C, the UE initiates a PDN Connection Session Establishment procedure. When the UAV needs to use an existing PDN connection for connectivity to the UAV-C, the UE initiates a PDN Connection Modification procedure. The UE shall include the following IEs in the PDN connection establishment/modification request: a CAA-Level UAV ID, a DNN/S-NSSAI implying dedicated connectivity to UAV-C, and UAV pairing information, which includes any needed authorization information, if available.

The pairing information includes the CAA-level UAV IDs of the requesting UAV and identification information of UAV-C to pair. The USS may also use its locally configured pairing information for UAV and UAV-C pairing authorization which takes precedence over UAV provided pairing information.

NOTE: The integrity protection of pairing information is recommended. It is performed by the USS, and is not in scope of 3GPP system.

2. The SMF+PGW-C determines whether the UAV pairing authorization is required based on UAV's aerial subscription, presence of CAA-Level UAV ID, and DNN/S-NSSAI indicating the UAV service:

 The SMF+PGW-C invokes the authorization procedure with the USS via UAS-NF. The USS will perform C2 authorization taking account of the included pairing information, which includes any needed authorization information, if available, the CAA-Level UAV ID, and GPSI etc.

 The USS informs the SMF+PGW-C via the UAS NF of the authorization results. The authorization information includes the IP address of the UAV-C and a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result, i.e., whether the UAV is allowed to be paired with the UAV-C) if the USS has such information to send. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope. The other information contained in this message is given in TS 23.256 [3].3. The SMF+PGW-C sends the UE the C2 authorization payload with the paring authorization result and may also send a new CAA-level UAV ID. The UE shall store the Pairing authorization result and authorization information.

The PDN Connection Establishment/Modification continues and completes as described in TS 23.256 [3].

The UAV pairing authorization can be revoked by the USS at any time.

Besides, the paired UAV-C can be replaced by a new UAV-C by the USS at any time.

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