**3GPP TSG-WG SA2 Meeting #145E S2-210abc1**

**17th May – 28th May 2021, Elbonia (revision of S2-210xxxx)**

**Source: Nokia, Nokia Shanghai Bell**

**Title: TS 23.256: Generic IE names for UUAA-SM**

**Document for: Approval**

**Agenda Item: 8.7**

**Work Item / Release: ID\_UAS / Rel-17**

*Abstract of the contribution:*

# 1 Introduction

This paper proposes changes in TS 23.256 clause 5.2.3 to address the Editor's Note that is present in clause 5.3.2.1 as below:

" Editor’s Note: The naming for the procedures and IEs, where needed, will be updated to make them generic (i.e. not specific to ID\_UAS)."

**Observation 1:** During the PDU session establishment the UE (UAV) can provide (step 0, Figure 5.2.3.2 -1) a CAA-Level UAV ID, optionally a USS address and a UUAA Aviation Payload. Now it is to be noted that, while the 3GPP network needs to understand the CAA-Level UAV ID and the USS address (e.g. to initiate UUAA-SM procedure or for USS discovery), the UUAA Aviation Payload is transparently sent to the USS.

**Proposal 1:** It is proposed to use "Service Level Identity" for CAA-Level UAV ID, "Authentication Server Address" for USS address. Also, it is proposed to clarify in the description text that the "UUAA Aviation Payload" is sent in a transparent container by the UE.

**Observation 2:** In step 1 of Figure 5.2.3.2 -1, the SMF includes a CAA-Level UAV ID, optionally a USS address and a UUAA Aviation Payload in the Nnef\_Auth\_Request. Here also the UUAA Aviation Payload is transparent.

**Proposal 2:** It is proposed to use "Service Level Identity" for CAA-Level UAV ID, "Authentication Server Address" for USS address. Also, it is proposed to clarify in the description text that the "UUAA Aviation Payload" is sent in a transparent Authentication Data container.

**Observation 3:** In steps 4 & 5, of Figure 5.2.3.2 -1, the response from USS contains UUAA result, optionally a new CAA-Level UAV ID and optionally an UUAA Authorization Payload. While 3GPP network needs to know the UUAA result and the new CAA-Level UAV ID, the UUAA Authorization Payload is transparently sent to the UE (UAV).

**Proposal 3:** It is proposed to use "Service Level Identity" for CAA-Level UAV ID, "Authorization Data" for UUAA Authorization Payload and clarify that the "Authorization Data" is transparently sent to the UE (UAV), similarly to the UUAA Aviation Payload.

**Observation 4:** In step 6 of Figure 5.2.3.2 -1, it is mentioned that the SMF receives the DN Authorization Profile Index and DN authorized Session AMBR in DN Authorization Data from the UAS NF/NEF. However, it is not clear how/when the UAS NF/NEF gets such information. This information should come from the USS in step 4. However, in step 4 it is only mentioned that the USS may include "requested policy information".

**Proposal 4:** It is proposed to clarify in step 4 that the USS may include the DN Authorization Profile Index and a DN authorized Session AMBR as part of the requested policy information.

**Observation 5:** In Clause 5.2.3.1, currently it is mentioned that UAV shall indicate in PDU session establishment/modification request if the session is used for UAV communication or C2 communication. However, it was agreed in SA2 #144E meeting that there is no need for an explicit indication from the UE (UAV).

"*The UAV shall indicate that the PDU Session/PDN Connection is for the UAV communication and/or C2 communication in the PDU Session Establishment/PDN Connectivity request.*"

**Proposal 5:** It is proposed to delete the above highlighted (*Italic*) text.

**Observation 6:** In the UUAA-MM procedure the UAV is referred to as UE (UAV). But in UUAA-SM procedure currently different terms are used like UE, UAV, UAV/UE etc.

**Proposal 6:** It is proposed to align the terminology with UUAA-MM procedure and use "UE (UAV)" throughout.

# 2 Proposal

It is proposed to approve the below content. All changes are marked with revision marks.

\* \* \* \* Begin of Changes \* \* \* \*

### 5.2.3 UUAA At PDN Connection/PDU Session Establishment (UUAA-SM)

#### 5.2.3.1 General

Editor’s Note: This procedure will be revisited after security aspects on UUAA are determined by SA3.

An UE (UAV) uses PDU Sessions or PDN Connections for connectivity with the USS and for connectivity with a networked UAV-C.

A networked UAV-C is a UE which uses existing procedures for establishing PDU Session or PDN Connection for communication with the USS/UTM, and the procedures described in this clause do not apply to a networked UAV-C.

This clause describes procedure that applies both for 5GS and EPS, where PDU Session refers to 5GS and PDN Connection refers to EPS.

PDU Session/PDN Connection for UAV communication shall only be established after a UAV has been authenticated and authorized by the USS this may happen during UUAA-MM, as described in clause 5.2.2, , or during UUAA-SM as described in this clause.

A UE (UAV) may use either a common or separate PDU Session/PDN connection for connectivity with the USS and a UAV-C.

When the UE (UAV) requests establishment of a PDU session/PDN connection, the PDU session/PDN Connection may require UUAA authorization, subject to operator, regulatory requirements as described in clause 5.2.4.

If the UE (UAV) uses the PDU session/PDN connection for C2 the PDU session is subject to C2 authorization as described in clause 5.2.5.

The PDU Session/PDN Connection is identified by the SMF/SMF+PGW-C as being for UAV/C2 communication based on the DNN or DNN/S-NSSAI combination.

During the establishment or modification procedure of the PDU Session/PDN connection for C2 communication, the USS shall provide the 3GPP system with following information for enabling basic C2 communication between UAV and UAV-C:

- traffic filters

- QoS requirements

The USS can enable/disable C2 communication between UAV and UAV-C necessary for services used during the flight operation at any point in time as described in clause 5.2.9.

Clause 5.2.3.2 defines the USS UAV Authorization/Authentication (UUAA) procedures at PDU Session Establishment in 5GS and clause 5.2.3.3 is for the PDN Connection Establishment in the Attach procedure for EPS using the interworking functionality.

When the UAV - UAV-C pairing authorization is revoked by the USS, the SMF or SMF+PGW-C shall release the PDU Session/PDN connection for C2 communication (in case separate PDU Sessions/PDN Connections are used), or disable C2 communication for the PDU Session/PDN connection (in case separate connections are used).

When the UUAA is revoked by the USS, all UAV related PDU Session/PDN connections shall be released.

#### 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 TS23.502 [3], clause 4.3.2.2 and additionally based on the SM subscription data obtained from UDM, and the Service Level 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 3GPP TS23.502[3] figure 4.3.2.2.1-1.

The SMF determines that it needs to invoke UAS NF/NEF service operation for Authentication/Authorization of the PDU session establishment request.

The UE (UAV) includes the the Service Level Identity (i.e. the CAA-Level UAV ID of the UAV) and may include the Authentication Server Address (i.e. the USS address) and optionally an Authentication Data with UUAA Aviation Payload in a transparent container in the PDU Session Establishment request.

NOTE 1: The definition of the contanier is for stage 3 to specify.

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

1. The SMF invokes Nnef\_Auth\_Request, including the Service Level Identity (that contains the CAA-Level UAV ID of the UAV), an Authentication Server Address (i.e. the USS address) if it was provided by the UE (UAV), the transparent Authentication Data container containing the UUAA Aviation Payload if it was provided by the UE (UAV), GPSI, PEI if available, and the UE IP Address.

The UAS NF/NEF selects a USS based on either CAA-Level UAV ID or the USS address as described in clause 4.4.2.

Editor's Note: How the 3GPP System shall handle an initial PDU Session Establishment Request from a UAV if UUAA has been performed at Registration is FFS.

2. From UAS NF/NEF to USS: N33\_Auth\_Request forwarding the authentication request received information from the SMF.

3. [Conditional] Multiple rount-trip messages as required by the authentication method used by USS. N33\_Auth\_Response messages from USS shall include GPSI and may include a authentication message based on authentication method used that is forwarded transparently to UE (UAV) over NAS MM transport messages.

4.

The USS sends N33\_Auth\_Response to the UAS NF/NEF with the Authentication/Authorization result containing the UUAA result, optionally a Service Level Identity containing the new CAA-Level UAV ID, requested policy information, a transparent Authorization Data container containing 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 2: The USS stores a mapping between CAA-Level UAV ID and the External Identifier. The External Identifier 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 etc.
The External Identifier and/or UAV IP Address can be used at a later point by the USS for 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 forwards the Authentication/Authorization result, a Service Level Identity containing the new CAA-Level UAV ID, if received from the USS, and the transparent Authorization Data container containing the UUAA Authorization Payload, if received from the USS, to the SMF.

6. The PDU Session establishment continues and completes. In the step 7b of the TS 23.502 [3] Figure 4.3.2.2.1-1, 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 TS 23.503 [20] clause 6.4) and the PCC rule(s) (described in TS 23.503 [20] clause 6.3) from the PCF. If the SMF receives the DN authorized Session AMBR 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 TS 23.503 [20] clause 6.4).

The SMF transfers the Authentication/Authorization result, the Service Level Identity containing the new CAA-Level UAV ID and the transparent Authorization Data container containing the UUAA Authorization Payload to the UE (UAV) as in step 11, 12 and 13 in 3GPP TS 23.502 [3] figure 4.3.2.2.1-1

NOTE 3: The definition of the container is for stage 3 to specify.

NOTE 4: If C2 information is available from USS during the initial PDU Session Establishment procedure the SMF can interact with the PCF to set up PCC rule(s) for the C2 communication.

#### 5.2.3.3 USS UAV Authorization/Authentication (UUAA) during default PDN connection at Attach

In the figure 5.2.3.3-1 two options are specified for the execution of the UUAA. Option 1 (i.e. step 2 in figure 5.2.3.3-1) can be used if the timing of the UUAA is not seen as an issue to perform the Attach procedure. Option 2 (i.e. step 4 and 6 in figure 5.2.3.3-1) has to be used if the timing for the UUAA is seen as too long and may have negative effects on the Attach procedure e.g. the Attach procedure can time-out before response have been received from USS.



Figure 5.2.3.3-1: UUAA during Attach procedure in EPS

0. Steps 1 - 13 in TS23.401 [5] figure 5.3.2.1-1 and steps 1 - 2 in TS23.502 [3] figure 4.11.1.5.2-1 or clause 4.11.2.4.1 in TS23.502 [3].
UE (UAV) sends Attach Request including the Service Level Identity (i.e. the CAA-Level UAV ID of the UAV), and may include the Authentication Server Address (i.e. the USS address) and optionally Authentication Data with the UUAA Aviation Payload in a transparent container, etc. in the PCO to the SMF+PGW-C.
The MME may determine the UAV has an aerial subscription and selects the Default APN for connectivity with the USS.

NOTE 1: The definition of the PCO field is for stage 3 to specify.

1. [OPTION 2] SMF+PGW-C configures an Access Control List (ACL) in UPF+PGW-U to stop any traffic over the default PDN Connection.

2. [OPTION 1] UUAA is performed as described in steps 1, 2, 4 and 5 in figure 5.2.3.2-1.

Editor's note: Optional step 2 in figure 5.2.3.2-1 is not supported in current release of EPC.

3. Steps 14 - 22 in TS23.401 [5] figure 5.3.2.1-1 and steps 3 - 6 in TS23.502 [3] figure 4.11.1.5.2-1 or clause 4.11.2.4.1 in TS23.502 [3].

4. [OPTION 2] UUAA is performed as described in steps 1, 2, 4 and 5 in figure 5.2.3.2-1.

5. Steps 23 - 24 in TS23.401 [5] figure 5.3.2.1-1.

6. [OPTION 2] The PCO including the Authentication/Authorization result and the transparent Authorization Data with UUAA Authorization Payload are transferred from SMF+PGW-C to UE (UAV) in Update Bearer Request and Downlink NAS Transport (step 6a - 6c). The UAV/UE confirms the update in steps 6d - 6f.

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