**3GPP TSG-SA3 Meeting #105e *S3-213924r6***

**e-meeting, 8 - 19 November 2021**  merger of 3924, 4126, 4162

**Source: Huawei, HiSilicon, Lenovo, Motorola Mobility, Qualcomm**

**Title: UUAA procedure during PDU session establishment**

**Document for: Approval**

**Agenda Item: 4.6 ID\_UAS**

# 1 Decision/action requested

***Approve the proposed pCR as normative text***

# 2 References

[1]

# 3 Rationale

This contribution proposes the UUAA procedure based on the agreed principle in the study. It is in-line with SA2’s procedure as well.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES (all text new) \*\*\*

### 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 during PDU Session Establishment

According to TS 23.256 Clause 4.2.1, if UUAA is not performed during the Registration procedure in 5GS, the UUAA is performed at PDU session establishment when the UAV requests user plane resources for UAV operation. If the UUAA has been performed successfully during registration, the AMF on receiving the PDU session establishment request with CAA-Level UAV ID checks if it has any valid UUAA results available for the corresponding CAA-level UAV ID and provides the valid UUAA results to the SMF along with the PDU session establishment request. If the SMF receives from AMF, a PDU session request message along with valid UUAA results for a CAA-Level UAV ID, then the SMF shall notperform another UUAA and it continues with steps 6-8 of PDU session establishment procedure specified in TS 23.256 Clause 5.2.3.2.

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 procecure 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 authorised USS shall be used in order to ensure only legitimate entities can provide authorisation 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. Whether Authentication messages are transmitted over EAP is determined by USS:

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: 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, C2 assistance information that indicates the pairing related information such as UAV-C ID (if the UE is not preconfigured), and a transparent container (which may contain UAS security information) to the UAV.

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

Editor's Note: Sending the Authentication Response message also allows UAS-NF to identify the USS, e.g. through sending the USS identifier in the Authentication Response message or based on other identification information exchanged through the interface between UAS NF and USS. Whether the identifier of the USS is sent will depend on the security solution chosen for the UAS NF to USS interface which is FFS.

Editor's Note: It is FFS, how the UAS data is protected if the user plane enforcement policy is set to preferred or not needed. As the USS has no knowledge of whether an UP IP will be applied or not by the 5GS for a specific UAS connection, it may end up with no security being applied for the UAS data.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).

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, C2 assistance information (if received) 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), C2 assistance information (if received) 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, C2 assistance information and UAS Security information.

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