**3GPP TSG-SA3 Meeting #105e *S3-213923r4***

**e-meeting, 8 - 19 November 2021**

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

**Title: UUAA procedure at registration**

**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

\*\*\* START OF 1st CHANGES (all text new) \*\*\*

### 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 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. 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. 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 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 responses 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.

NOTE: 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 and the content of Auth Message 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 may contain UAS security information.

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.

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: If the UUAA happens during Registration, then UUAA will not happen during the following PDU session establishment procedure. In such scenario, it is FFS, how the UAS data is protected if the userplane 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 and it is also expected that sending any UAS security information is ‘optional’, it may end up with no security being applied for the UAS data finally.

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

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), and the UUAA Authorization Payload received in step 5. The message(s) used in step 7 and any further actions the AMF takes 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 UE shall store the result, the authorization information and if receivedUAS Security information along with the CAA-level UAV ID.

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