**3GPP TSG-SA3 Meeting #104e ad-hoc *S3-213367r1***

**e-meeting, 27 - 30 September 2021** Merger of S3-213367, S3-213517, S3-213558

**Source: Huawei, HiSilicon, InterDigital, Qualcom, Lenovo, Motorola Mobility**

**Title: UUAA procedure at registration (5G)**

**Document for: Approval**

**Agenda Item: 4.7 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. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]). For an AMF initiated re-authentication, the procedure starts from the step 2.



Figure 5.2.1.2-1: UUAA Procedure at Registration

Editor's Note: The figure needs to be aligned with steps.

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 a transparent container including the Aviation Payload if provided by the UE. The AMF may include other information in the request (see TS 23.256 [3]).

Editor's Nnote: Whether the transparent container is delivered to the USS based on the EAP/Diameter mechanism or an API-based mechanism is FFS.

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 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:

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 received in 4a tothe 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 including the Authentication message 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 Auth Message are out of scope of 3GPP.

Editor's Note: If multiple authentication methods are supported, it is FFS how an authentication method is negotiated/selected. If only one authentication method is supported, the details of steps 4a-4b will be updated accordingly.

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, the USS Identifier, and a transparent container composed of Authorization Payload to the UAV. Optionally, the Authentication Response may include a new authorized CAA-level UAV ID.

Editor's Note: Whether CAA-level UAV ID is needed from a security perspective is FFS.

Editor's Note: Whether the USS identifier is sent to the UAS NF will depend on the security solution chosen for UAS NF to USS interface.

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).

The transparent container contains UAS security information. The content of security information (e.g. key material to help establish security between the UAV and USS/UTM) is not in 3GPP scope.

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 transparent container received in step 5.

7. The AMF sends to the UE the UUAA result (success/failure) and the transparent container 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

Editor's Note: Whether CAA-level UAV ID is needed from a security perspective is FFS.

\*\*\* END OF 1st CHANGES \*\*\*

\*\*\*\* START OF 2nd CHANGES \*\*\*\*

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: “Security architecture and procedures for 5G system”

[3] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".

[4] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

\*\*\*\* END of 2nd CHANGE \*\*\*\*