**3GPP TSG-SA3 Meeting #104-e *S3-212584r2***

**e-meeting, 16 - 27 August 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon, InterDigital**

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

**Document for: Approval**

**Agenda Item: 4.20 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) \*\*\*

### X.x.x.3 UUAA Procedure during PDU Session Establishment

The SMF may trigger a UUAA procedure during the PDU session establishment procedure with details described below. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [aa]).

1. The SMF determines the UUAA procedure as described in the clause X.x.x.1, where the UE may provide a CAA-Level UAV ID indicating UAS services and optionally a transparent container composed of the UUAA Aviation Payload in the PDU Session Establishment request. The SMF triggers a UUAA procecure after the determination in step 7 in the clause X.x.x.1.

2. The SMF 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 SMF may include other information in the request (see TS 23.256 [aa]).

Editor's note: 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 which includes the GPSI, the CAA-Level UAV ID and the transparent container. Other information may be included in this message (see TS 23.256 [aa]).

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 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 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.

If UUAA successful, the UAS NF stores the UAV UEs’ UUAA context, includes 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

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 or an identifier local to the UAS NF is FFS

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, and the transparent container received in step 5.

The SMF stores the results, together with the GPSI and the CAA-level UAV

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

7. The SMF sends the UUAA result (success/failure) and transparent container received in step 5 to the UE. The message(s) used in step 7 and and any further actions the SMF takes are given in TS 23.256 [aa].



Figure X.x.x.3-1: UUAA Procedure during PDU Session Establishment

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

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