**3GPP TSG-SA3 Meeting #104e ad-hoc *S3-213370r4***

**e-meeting, 27 - 30 September 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: UUAA re-authentication procedure (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 re-authentication 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 are new) \*\*\*

### 5.2.1.4 UUAA re-authentication procedure (5G)

As described in 5.2.1.1, the USS or the AMF (if support UUAA during registration) may initiate the Re-authentication procedure for the UAV at any time.

This clause describes the USS initiated Re-authentication procedure (the AMF initiated Re-authentication procedure is described in the clause 5.2.1.2). The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).



Figure 5.2.1.4-1: UUAA re-authentication in 5GS

1. The USS sends a re-authentication request for the UAV to UAS-NF that includes GPSI, CAA-Level UAV ID, and an Authentication message. It may contain the PDU Session IP address if available.

Editor's Note: For USS initiated re-authentication, how the USS/UTM contacts the right UAS NF which stores the UUAA context corresponding to an UAV is FFS

Editor's Note: Inclusion of CAA-Level UAV ID and PDU Session IP address is FFS

Editor's Note: Sending the re-authentication request also allows UAS-NF to identify the USS, e.g. through sending the USS identifier in the request 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

2. The UAS NF retrieves the UAV UE's context. The UE’s context contains identity mapping between the GPSI and the USS identifier that performed UAA. The UAS-NF verifies the USS re-authentication request by checking whether the GPSI and the USS identifier match the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the re-authentication procedures if match.

The UAS NF determines whether the target NF is an AMF or an SMF.

* If the target NF is an AMF, the UAS NF further determines the target AMF for re-authentication and continues step 3a.
* If the target NF is an SMF, the UAS NF further determines the target SMF for re-authentication and continues step 3b.

3a or 3b. The UAS NF sends to either the target AMF or the target SMF the UAA re-authentication request for the UE identified by the GPSI and for the SMF only the PDU Session IP address if available.

4. The UAS NF responses the USS that the UAA Re-authentication has been initiated.

5a. If the target NF is an AMF, the AMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.2 (step 2 to step 9).

5b. If the target NF is an SMF, the SMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.3 (step 2 to step 7).

Editor's Note: It is FFS, how in step 2 and step 5a and 5b, the AMF/SMF triggers UUAA with the UE related to the re-authentication initiated by the USS

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