**3GPP TSG-SA3 Meeting #102bis-e *S3-210976r1***

**e-meeting, 1 – 5 March 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: pCR – Add evaluation to solution 1**

**Document for: Approval**

**Agenda Item: 2.7**

# 1 Decision/action requested

***Approve this contribution to add evaluation for solution 1***

# 2 References

[1]

# 3 Rationale

The contribution add in evaluation text to solution 1.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES \*\*\*

## 6.1 Solution #1: UAS authentication and authorization

### 6.1.1 Solution overview

This solution address the key issue #1.

This solution assumes each UAV or UAVC is provisioned with a PLMN UE ID (SUPI) and the corresponding credential so that it can be authenticated (primary authentication) by the PLMN as a normal UE. In addition, UAV or UAVC is provisioned with a UAS ID and corresponding credentials to perform UAS authentication and authorization (UAA) with USS/UTM.

The UAA is mandatory for UAA or UAVC and is based on EAP framework, where AMF is taking the role of the transparent Authenticator.

### 6.1.2 Solution details

#### 6.1.2.1 Registration

The call flow of this solution is shown in the figure below.



**Figure 6.1.2.1-1: UAA procedure**

1. UAV (or UAVC) sends registration request to AMF. It may indicate that this is a registration for UAS.

 NOTE: a new IE or an extension of an existing IE can be used to indicate UAA is requested. The IE can be defined in stage 3 and in coordination with CT.

2. AMF initiates Primary authentication as a normal UE

3. After successful Primary authentication, AMF checks whether UAV (or UAVC) requires UAA. This may be based on the subscription information retrieved from UDM in step 2

4. AMF returns a Registration Accept message to the UAV and indicates that UAA is pending.

5. UAA starts with EAP message exchanges.

 a. AMF may optionally request UAS ID from UE.

b. UAV (or UAVC) responses with UAS ID. It may indicate whether this is a UAV or UAVC.

c. AMF sends UAA requests to UFES (as defined in TR 23.754 [3]) with UAS-ID and UAV or UAVC indicator in the EAP message. In addition, UAA request contains GPSI for USS/UTM to identify the UAV. GPSI shall be bound to UAS-ID. UFES locates the corresponding USS and forwards the UAA requests to it.

d. USS/UTM response with EAP messages to AMF through UFES accordingly

e. EAP messages may continue based on the EAP method used.

f. …

Note: the EAP authentication method used by UTM is out of scope of 3GPP

6. Based on the EAP authentication outcome, USS/UTM sends the results to AMF through UFES. If successful, USS/UTM sends the EAP-Success message, together with UAV/UAVC’s GPSI and UAS-ID that can uniquely identity the UAV/UAVC.

7. AMF stores the results, together with SUPI (converted from GPSI), UAS-ID, and UAV/UAVC indicator

8. AMF triggers the UE Configuration Update procedure. The message AMF sent to UE includes the UAS-ID and may include an indication it is for a UAV (or UAVC), if needed.

#### 6.1.2.2 Revocation

USS/UTM may trigger revocation of UAA at any time. The call flow is shown in the figure 6.1.2.2-1.



Figure 6.1.2.2-1: UAA revocation procedure

1. The USS/UTM sends the UAA revocation request to AMF through UFES to revoke the UAS service for a UAV. The UAV is identified by the GPSI and UAS-ID in the UAA revocation Request.

NOTE: UFES is an NF interfacing USS/UTM and it can locate AMF serving the UAV.

2. The AMF may inform UAV with the UAA revocation message.

3. The AMF responses USS that the UAV’s authentication and authorization is revocated.

4. The network may deregister the UAV if needed, as per current procedure.

### 6.1.3 Solution evaluation

This solution addresses the key issue #1 (the fourth requirement for the fake USS/UTM has not addressed).

In this solution, each UAV is assumed to be provisioned with UE ID (i.e. SUPI by PLMN) as well as UAS ID (by USS/UTM), together with corresponding credentials for authentication. The UAS authentication and authorization (UAA) with USS/UTM is performed after UAV is authenticated with the network (using UE ID).

This solution supports multiple UAA methods to meet potential different authentication requirements from USS/UTM. EAP framework can be used to carry the UAA messages.

This solution supports revocation triggered by USS/UTM at any time.

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