**3GPP TSG-SA3 Meeting #102bis-e *S3-210977r1***

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

**Source: Huawei, HiSilicon**

**Title: pCR – Add evaluation to solution 11**

**Document for: Approval**

**Agenda Item: 2.7**

# 1 Decision/action requested

***Approve this contribution to add evaluation text for solution 11***

# 2 References

[1]

# 3 Rationale

The contribution add in evaluation text to solution 11.

# 4 Detailed proposal

pCR

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

## 6.11 Solution #11: UAV and UAVC pairing authorization through bound IDs

### 6.11.1 Solution overview

This solution addresses the key issue #2: Pairing authorization for UAV and UAVC.

This solution assumes UAV and UAVC are equipped with SUPI and credentials from PLMN. The pairing authorization is performed after UAV or UAVC is authenticated by 3GPP systems through Primary authentication. It is performed when UAV is being authenticated/authorized, or after it has been authenticated/authorized by USS/UTM.

### 6.11.2 Solution details

#### 6.11.2.1 UAV and UAVC pairing authorization

A general overview of the procedure involving UAV and UAVC paring authorization is shown in Figure below.



Figure 6.11.2.1-1: A general overview on UAV and UAVC pairing authorization

0. Provisioning:

a. UAV and UAVC: provisioned with UAV IDs and corresponding credentials, e.g. their private/public key pairs and certificates issued by UAS service providers/operators. Regarding pairing, there are two options considered: 1) provision is not required, it will be provisioned at USS/UTM 2) pairing is provisioned at both UAV and UAVC, e.g. indicated using certificates.

b. USS/UTM: provisioned with its private/public key pairs. The UAS service providers/operators have registered their public keys or their root CAs with USS/UTM so that USS/UTM can verify their issued certificates. Regarding pairing, similarly, there are two options: 1) pairing of UAV and UAVC has been provisioned and UAV-ID and UAVC-ID are bound together; 2) no pairing information provisioned.

NOTE 1: UAV and UAVC pairing shall not be determined by other parties than USS/UTM or UAS itself, e.g. between UAV and UAVC. The provisioning is out of scope of 3GPP.

1. Primary Authentication: UE1 (UAV) and UE2 (UAVC) are equipped with SUPI and 3GPP credentials and need to perform Primary Authentication as normal UEs before getting UAS services.

2. For UAS-type UE, UAS authentication is performed for UAV.

NOTE 2: UAV authentication is not addressed in this solution. This steps is to indicate pairing is for authenticated and authorized UAV.

3. USS/UTM authorize UAV and UAVC pairing

a. Case 1 (pairing information is provisioned at USS/UTM): based on bound UAV-ID and UAVC-ID to determine whether pairing request from UAV (with UAV-ID and GPSI) or UAVC (with UAVC-ID and GPSI) can be authorized.

b. Case 2 (UAV-ID and UAVC-ID are paired and bound): based on bound information sent from UAV or UAVC to determine whether pairing request from UAV (with UAV-ID and GPSI) or UAVC (with UAVC-ID and GPSI) can be authorized. USS/UTM may need to verify the certificates presented by UAV/UAVC.

NOTE 3: UAV (or UAVC) does not send GPSI to AMF. Instead, it sends UE ID (e.g. GUTI or SUCI) as a normal UE and AMF will convert the UE ID into GPSI.

3-1. UAV sends a pairing request message, e.g. in a PDU Establishment Request message to USS through the network (e.g. AMF or SMF and UFES). The message will include UAV-ID and its UE ID (e.g. GUTI). For Case 2, it includes UAV-ID (and UE ID if available) of the paired UAVC as well.

3-2. USS determines whether to authorize the pairing of UAV and UAVC

3-3. USS informs PLMN and UAV the authorization results. The message includes UAV-ID and GPSI of the UAV. and It may include the UAVC-ID and GPSI of the paired UAVC if available. Based on the results, the PLMN (e.g. SMF) may determine whether the PDU session is authorized for UAV and UAVC communications.

NOTE 4: step 3 and step 2 may be combined depending on scenarios.

4. UAVC communicates with UAV through UPF (UP).

#### 6.11.2.2 Revocation

USS/UTM may trigger revocation pairing of UAV and UAVC pairing at any time. The call flow is shown in the figure 6.11.2.2-1.



Figure 6.1.2.2-1: UAS pairing revocation procedure

1. The USS/UTM sends the UAA revocation request to SMF through UFES to revoke the UAVC pairing for a UAV. The UAV and UAVC are dentified by their GPSI and UAS-ID respectively in the UAA revocation Request.

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

2. The SMF may inform UAV or UAVC with the UAA pairing revocation message.

3. The SMF responses USS that the pairing of UAV and UAVC has been revocated.

### 6.11.3 Solution evaluation

This solution addresses the key issue #2.

In this solution, pairing information is assumed to be pre-provisioned, 1) provisioned at USS/UTM; 2) provisioned at UAV/UAVC (the provisioning is not scope of 3GPP). Pairing authroization is performed at USS/UTM after UAV is authenticated by PLMN. Pairing authorization is sent to PLMN with associated IDs (e.g. GPSI and/or UAV IDs).

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

Editor's note: Further evaluation is ffs on SMF enforcing authorization of C2 traffic

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