**3GPP TSG-SA3 Meeting #105e *S3-213925r1***

**e-meeting, 8 – 19 November 2021** Revision of S3-20xxxx

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

**Title: Pairing Authorization**

**Document for: Approval**

**Agenda Item: 4.6 ID\_UAS**

# 1 Decision/action requested

***Approve the proposed pCR as normative text***

# 2 References

[1]

# 3 Rationale

This contribution proposes the Pairing Authorization 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.X Pairing Authorization for UAV and UAVC

### 5.X.1 General

Pairing authorization in 5GS is performed during either a PDU Session Establishment procedure or a PDU Session Modification procedure.

Editor's Note: UAV pairing authorization during PDU Session Modification is FFS.

### 5.X.2 UAV pairing Authorization with UAVC in 5GS

Pairing authroization may be performed during a PDU Session Establishment after a successful UAA between the UAV and the USS/UTM.

UAV pairing authorization during the PDU session establishment procedure is described as follows. Full details of the procedures are given in TS 23.256 [3].



Figure 5.X.1-1: UAV pairing authorization during PDU Session Establishment

1. When the UAV needs a new dedicated PDU session for connectivity to the UAV-C, the UE initiates a PDU Session establishment procedure. The UE shall include the following IEs in the PDU session establishment/modification request: a CAA-Level UAV ID, a DNN/S-NSSAI implying dedicated connectivity to UAV-C, authorization information, and UAV pairing information if available.

The pairing information includes the CAA-level UAV IDs of the requesting UAV and identification information of UAV-C to pair. The USS may also use its locally configured pairing information for UAV and UAV-C pairing authorization which takes precedence over UAV provided pairing information.

NOTE: The integrity protection of pairing information is recommended. It is performed by the USS,and is not in scope of 3GPP system.

2. The SMF determines whether the UAV pairing authorization is required based on UAV’s aerial subscription, presence of CAA-Level UAV ID, and DNN/S-NSSAI indicating the UAV service, as step 7 in clause 5.2.1.1.

The SMF invokes the authorization procedure with the USS via UAS-NF. The USS will perform C2 authorization taking account of the included pairing information, the CAA-Level UAV ID and GPSI etc.

The USS informs the SMF via the UAS NF of the authorization results. The authorization information includes the IP address of the UAV-C and a transparent container which may contain UAS security information. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope. The other information contained in this message is given in TS 23.256 [3].

3. The SMF informs the UE the paring authorization result in the PDU Session Accept message, which includes a new CAA-level UAV ID. The UE shall store the Pairing authorization result and authorization information.

The PDU Session establishment continues and completes as described in TS 23.256 [3].

The UAV pairing authorization can be revoked by the USS at any time.

Besides, the paired UAV-C can be replaced by a new UAV-C by the USS at any time.

Editor's Note: It is FFS, how the C2 data is protected if the user plane enforcement policy is set to preferred or not needed. As the USS has no knowledge of whether a user plane protection will be applied or not by the 5GS for a specific C2 connection, it may end up with no security being applied for the C2 data.

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