**3GPP TSG-SA3 Meeting #100bis-e *S3-202388***

**e-meeting, 12 - 23 October 2020** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: pCR – A solution to C2 communication security**

**Document for: Approval**

**Agenda Item: 2.7**

# 1 Decision/action requested

***Approve this contribution to add a solution in TR33.854***

# 2 References

[1]

# 3 Rationale

The contribution proposes a solution to address KI #7: Security of Command and Control (C2) Communication

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES (all text are new) \*\*\*

## 6.X Solution #X: C2 communication security in application layer

### 6.X.1 Solution overview

This solution addresses the key issue #7: Security of Command and Control (C2) Communication.

This solution proposes an end-to-end security, e.g. confidentiality, integrity protection, relay protection, and non-repudiation, at the application layer to complement security mechanisms available in the 3GPP system. While the specific security method used in the application layer is out of scope of 3GPP, some information exchange facilitated by the 3GPP system is needed.

### 6.X.2 Solution details

It is assumed that C2 communication is based on PDU sessions between a UAV and UAVC. The secuirty setup is performed before or during PDU session establishment. As the PDU session establishment procedure has not been concluded, the call follow is illustrated as follows:

1. UAV (or UAVC) sends registration request.
2. UAV and UAVC are authenticated and authorized. This includes, where applicable, Primary Authentication, UAA by USS/UTM, UAV and UAVC pairing authorization, and/or flight authorization.
3. USS/UTM generates C2 session keys. USS/UTM may include information received from step 2 to generate the session keys, e.g. UAS-IDs/GPSI of UAV.
4. USS/UTM send a session key to UAV and UAVC respectively. The transmission needs to be secured, e.g. encrypted or integrity protected using UAV/UAVC public keys or session keys established between UE and USS/UTM etc.

NOTE: This step may be performed during or after step 5, if PDU authentication/authorization or PDU session establishment is required for the session key transmission.

1. C2 PDU session establishment procedure.
2. C2 communications using the session keys at step 4.



Figure 6.X.2-1: C2 security call flow

### 6.X.3 Solution evaluation

TBC

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