**3GPP TSG-SA3 Meeting #103-e *S3-211607r2***

**e-meeting, 17 – 28 May 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: pCR – Evaluation of solution #5**

**Document for: Approval**

**Agenda Item: 5.7 FS\_UAS\_SEC**

# 1 Decision/action requested

***Approve the proposed text evaluating solution #5 for TR33.854***

# 2 References

[1]

# 3 Rationale

This contribution proposes to add evaluation text to solution #5.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF 1st CHANGES \*\*\*

### 6.5.3 Solution evaluation

This solution is aligned with TR 23.754 conclusions for UUAA and pairing authorization using a PDU Session establishment/modification procedure, including the usage of a generic (API based) procedure via a UAS NF.

This solution fully addresses all requirements of Key Issue #1:

- The solution uses a generic (i.e., API based) procedure for secondary authentication of UAV by USS/UTM during PDU Session establishment (i.e., in addition to primary authentication). The UE provides its CAA-level UAV ID in the PDU Session establishment request to indicate it wants to access UAS services. The SMF triggers UUAA via a Proxy A&A (UAS NF), if the UE has a valid Aerial subscription. The authentication method and authentication messages content used during UUAA are in not in 3GPP scope.

- The solution enables the revocation of UAV authorization by the USS/UTM function via the UAS NF. The revocation may trigger a corresponding PDU Session release.

- Authentication of USS/UTM is handled by the Proxy A&A function by means of provisioned aviation domain certificates. USS/UTM address may be obtained from the UE or from a trusted resolution function which provides a USS/UTM address based on a CAA-level UAV ID.

This solution fully addresses all requirements of Key Issue #2:

- The solution enables UAV and UAV-C pairing authorization by USS/UTM. The pairing authorization is requested from USS/UTM during a PDU Session establishment/modification procedure. When pairing authorization is granted by USS/UTM, the SMF configures the PDU Session to allow C2 communication based on UAV-C peer connectivity authorization information provided by USS/UTM.

- Revocation of pairing follows similar principles as for UAV authorization revocation.

This solution fully addresses all requirements of Key Issue #6:

- The solution enables the transport of security information (e.g., token, key material) from the USS/UTM to the UE to secure communications between UAV and USS/UTM. The transport of the security information is enabled during a PDU Session establishment procedure (with UUAA). The content of the security information is not in 3GPP scope.

This solution fully addresses all requirements of Key Issue #7:

- The solution enables the transport of security information (token, key material) from the USS/UTM to the UE to secure C2 communications with UAV-C or USS/UTM. The transport of the security information is enabled during a PDU Session establishment/modification procedure (with UUAA and/or pairing authorization). The content of the security information is not in 3GPP scope.

~~Editor’s Note: Further evaluation is FFS for usage of generic (i.e. API based) authentication and authorization procedure compared to EAP mechanism~~

~~• As opposed to a solution based on the EAP framework,~~

API based procedure introduces a new mechanism compared to existing EAP framework. NOTE: Usage of API based is used to address an explicit requirement from the UTM community

NOTE: How and whether to protect the transparent containers used for UAV-USS communication during UUAA will be determined during the normative phase

NOTE: IETF/3GPP protocols are readily available for EAP based mechanism to protect the transparent containers.

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