**3GPP TSG-SA3 Meeting #100bis-e *S3-202635-r5***

**e-meeting, 12 - 16 October 2020** Revision of S3-202635

**Source: Ericsson**

**Title: pCR – A new solution for UAS authentication and authorization**

**Document for: Approval**

**Agenda Item: 2.7**

# 1 Decision/action requested

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

# 2 References

[1] TR 33.854: Study on security aspects of Unmanned Aerial Systems (UAS).

# 3 Rationale

This contribution proposes a solution for authentication and authorization of UAS raised in the key issue #1 in [1].

# 4 Detailed proposal

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

## 6.X Solution #X: UAS Authentication and Authorization using User Plane

### 6.X.1 Solution overview

This solution addresses the key issue #1. It introduces a new 3GPP AF (UAS AF) which validates that the UAV/networked-UAVC (networked-UAVC is the UAVC connected via 3GPP) has a valid UAV subscription and includes relevant UAV subscription information and UAV application information to be sent to the USS/UTM to support the USS/UTM for the authentication and authorization of the UAV/networked-UAVC. Throughout this key issue, unless otherwise specified, “UAVC” is used for “networked-UAVC”.

This solution assumes that each UAV or UAVC is provisioned with a PLMN UE ID and the corresponding credentials to be used in primary authentication by the PLMN as a normal UE. Also, the UEs are provisioned with a CAA level ID and corresponding credentials to be used in UAS authentication and authorization (UAA) by USS/UTM. The credentials used in UAS AA and AA method are out of 3GPP scope.

### 6.X.2 Solution details

The authentication and authorization procedure is presented in Figure 6.X.2-1.



Figure 6.X.2-1: UAA procedure

1. Primary authentication is performed.

2. A PDU session is established for the UE’s A&A request. The connection is allowed only between UAV/UAVC and UAS AF.

NOTE 1: The default policy for the PDU session on activation is to block any traffic from the UE except to the UAS AF.

NOTE 2: UAV/UAVC may want to connect to a DNN other than USS/UTM for some needs such as software updates. These type of PDU session request are out of this solution’s scope.

3. UAV/ UAVC sends the request for authentication and authorization to the UAS AF over the user plane, e.g. including UAV/UAVC identity, USS/UTM identity (if available), etc.

4. The UAS AF gets the relevant subscription information from PCF or UDM with support from existing BSF functionality.

Editor’s Note: It is FFS whether the proposed AF is a CP NF or a mixed CP+UP NF (no CP UP separation).

5. UAS AF checks if the UAV has a valid aerial subscription based on the subscription information received from UDM. The UAS-AF learns the 3GPP UAV ID/GPSI from the BSF lookup and adds it to the CAA-Level UAV-ID information that is forwarded to the USS/UTM.

NOTE 3: Correlation of the 3GPP UAV ID and CAA-Level UAV-ID is performed by the USS/UTM.

 If the check is successful, the UAS AF determines the USS/UTM serving the UAV/UAVC based on the USS/UTM identity provided in the request in Step 3 and the predefined list stored in UAS AF with valid USS/UTM identities including URLs to corresponding requests. If the requested identity is not in the list, the request from the UAV will be rejected. Otherwise, UAS AF sends AA request towards the UTM/USS. The UAS AF can include information to the USS/UTM needed for further interaction between USS/UTM and 5GS regarding the PDU session. The request can contain an indication about the used mobile operator and 3GPP UAV/UAVC identity. Additionally, it forwards also the UAV/UAVC specific information received in the UAS AA request.

Editor’s Note: The security of the interface between UAS AF and USS/UTM is FFS.

6. An authentication and authorization procedure is executed between UAV/UAVC and USS/UTM. USS/UTM considers the combined information from the UAV/UAVC and from the mobile network operator of the UAV/UAVC while performing the procedure.

NOTE 4: The credentials and the method used in the UAS AA are out of 3GPP scope.

Editor’s Note: Details of what information and how it is provided by MNO during the authentication and authorization procedure between UAV/UAVC and USS/UTM are FFS.

Editor’s Note: The details of secure message exchanges between UE and USS/UTM in order to support A&A by USS/UTM (e.g. EAP or other framework/mechanism) is FFS.

7. USS/UTM sends UAS AA result to UAS AF. If the AA is unsuccessful, USS/UTM may inform the UAS AF about the action to take e.g. whether the PDU session established in Step 2 will be terminated.

Editor’s Note: It is FFS whether USS/UTM is able to inform 3GPP about the action to be taken.

8. If the result of the AA in Step 6 is successful, the UAS AF informs the SMF to modify the PDU session established in Step 2 such that the UAV/UAVC can communicate to the USS/UTM.

 If AA is not successful in Step 6, the UAS AF may inform the SMF to terminate the PDU session established in Step 2 according to the response from USS/UTM in Step 7.

NOTE 5: This solution does not address UAS communication security.

NOTE 6: This solution does not enable/support authorization of UAV and UAVC pairing.

### 6.X.3 Solution evaluation

This solution requires a new function (UAS AF).

Editor’s Note: The impacts related to introducing UAS AF is FFS.

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