**SA WG2 Meeting #140e *S2-200xxxx***

**19 August – 02 September 2020, e-meeting (revision of S2-200xxxx)**

**Source: InterDigital**

**Title: Update to Solution #5: UAV authentication and authorization by USS/UTM based on NAS supplementary and secondary authentication and authorization procedures**

**Document for: Approval**

**Agenda Item: 8.7**

**Work Item / Release: [FS\_ID\_UAS] / [Rel-17]**

*Abstract: This contribution proposes an update to solution #5*

# 1. Discussion

This contribution proposes to clear to following ENs:

Editor's note: The exact format of the CAA-level UAV ID is FFS.

Editor's note: It is FFS whether the UAV can remain registered in 3GPP system if the UUAA fails.

Editor's note: The details of the 3GPP system awareness of the UAV and UAV controller pairing are FFS and depend on how the 3GPP system controls such connectivity. E.g. the PDU session or PDN connecting may be established initially enabling only user traffic between the UAV and the USS/UTM/UFES, and connectivity with the UAV controller is enabled only after the pairing is authorized by the USS/UTM, with appropriate traffic filters installed.

Editor's note: Whether a UAV controller control one or more UAV(s) is FFS and depends on discussion on architectural assumptions.

Editor's note: It is FFS whether the UAV can still use the PDN connection/PDU session if pairing authorization/authentication fails.

Editor's note: Which entity allocates a 3GPP UAV ID and how is used in the 3GPP network is FFS.

Editor's note: Whether any UAV-specific information is provided by the UAV is FFS

Editor's note: Whether the "pending UUAA" restricts the UAV from establishing any connectivity or only connectivity for UAS services is FFS.

Editor's note: It is FFS whether the AMF stores or processes the UAV authorization response information or simply provides the information to the UAV.Editor's note: Whether any UAV-specific connectivity configuration information is provided to the UAV by the AMF, and how such information is used in other steps, is FFS.

# 2. Proposal

It is proposed to capture the following solution proposal in TR 23.754.

**\* \* \* \* First Change \* \* \* \***

## 6.5 Solution #5: UAV authentication and authorization by USS/UTM based on NAS supplementary and secondary authentication and authorization procedures

### 6.5.1 Introduction

This solution addresses Key Issue #1, #2, #3 and #7.

This solution is applicable to EPC and 5GS.

This solution enables a:

- USS UAV Authorization/Authentication (UUAA) to ensure the UAV has successfully registered with USS/UTM and has therefore been authorized for operations by USS/UTM.

NOTE: The same functionality can be applied to a networked UAV Controller.

- Authorization of UAV and UAV controller pairing.

- Flight path authorization/registration for flight operation.

### 6.5.2 Functional Description

#### 6.5.2.1 Assumptions

The UAV is assigned a CAA-level UAV ID at the time of registration with the USS to be able to identify itself to the USS. The CAA-level UAV ID is assumed to uniquely identify the UAV at least within the scope of the USS to enable the CAA-level UAV ID correlation to UAV registration data by authorized Remote ID clients. The CAA-level UAV ID may also identify the assigning USS where it is listed. Based on local regulations, the CAA-level UAV ID may be static (e.g., serial number) or dynamic (e.g., session id). However, a consistent format for CAA-level UAV ID (either static or dynamic) is assumed when sent to the Remote ID USS or when broadcasted. The UTM/USS may also provide security credentials if USS UAV Authorization/Authentication (UUAA) option is used between the UAV and the UTM/USS when the UAV registers with the 3GPP network

Editor's note: Whether security credentials are also assigned with the CAA-level UAV ID or not is to be defined in SA3 or outside 3GPP.

It is assumed that the UE is assigned an External Identifier to be used for aerial operations as part of the Generic Public Subscription Identifier (GPSI), as described in clause 5.9.8 of TS 23.501 [12] and defined in TS 23.003 [14]. The External Identifier is used for interaction with external functions such as the USS.

NOTE: It is assumed that an MSISDN is not used as GPSI for the subscription corresponding to the UAV.

Both the scenario where the USS has a-priori relationship with the MNO and assigns the External Identifier corresponding to the SUPI, and the scenario where the USS is chosen dynamically without any a-priori association between the USS and the MNO must be supported. In the second case, the MNO is expected to assign External Identifiers for each aerial subscription according to an MNO specific mechanism, and such External Identifiers are expected to be communicated to the USS during the interaction between the UAV and the USS or between the MNO and the USS, as described below. We cannot assume the External Identifier is known to the USS, since the USS is not part of assigning the External Identifier for a UAV subscription and we cannot assume a close relationship between the MNO and the USS.

A UAV Flight Enablement Subsystem (UFES) may be used in the 3GPP system. The role of the UFES is to provide a single interface to the USS, thus limiting the impacts to the 3GPP system. Principally, the UFES performs the USS selection without requiring 3GPP network nodes (e.g. AMF, SMF in 5GC, or PGW in EPC) to implement such USS discovery mechanisms. The UFES supports delivery of the UAV External Identifier as 3GPP UAV ID to the USS, and can retrieve relevant subscription information from UDM and/or receive policy control by the PCF. USS selection by the UFES is based on the CAA-Level UAV ID, as described in this solution, and neither on UDM subscription information nor PCC policy.

Editor's note: Multiple UFES may be deployed in the network, thus how UFES is selected by SMF is FFS. Whether a USS interconnects with multiple UFESs or a UFES interconnects with multiple USS(s) is FFS.

Editor's note: Whether the functionality of UFES is a standalone NF or part of NEF is FFS.

#### 6.5.2.2 Overview of the Solution

In order to address the various aspects of authentication and authorization of UAS in the 3GPP system, the solution introduces the following building blocks:

1. UAS operator (i.e. the owner of the UAS) performs a procedure to register the UAS with the UTM/USS. 3GPP does not focus on the detail of this procedure. It is assumed that the registrant provides aviation-level information (e.g. UAV Serial Number, pilot information, UAS operator, etc.), whose content is dependent on the CAA and specific geography. This procedure may happen offline or via 3GPP Internet connectivity. During this step, the UAV is assigned a CAA-Level UAV ID. USS may or may not be involved.

2. UE primary authentication: the UAV is authenticated by the 3GPP system using the MNO credentials.

3. USS UAV Authorization/Authentication (UUAA): a UAV 3GPP authentication/authorization may be performed by the CN when the UAV accesses the 3GPP system to ensure the UAV has successfully registered with USS/UTM and has therefore been authorized for operations by USS/UTM. The UUUA is triggered by the 3GPP CN based on subscription and local policies, the final decision to authorize the UAV is made by the USS/UTM, and the CN receives confirmation of the authorization from USS. If the UUAA fails, the network may keep the device registered in the 3GPP system or deregister it based on the network policy. If the network keeps it registered, the network should disable the UAV related functionalities for the device.

4. Authorization of UAV and UAV controller pairing: the pairing between the UAV and the UAV controller for the use of UAV3 may be at least authorized, or even authenticated, by the USS/UTM, and not by the 3GPP system. The authorization/authentication is between the UAV and the USS/UTM, however the results are made known to the CN in order to enable the USS/UTM to enable the connectivity between the UAV and the UAV controller.

Editor's note: The details of the 3GPP system awareness of the UAV and UAV controller pairing are FFS and depend on how the 3GPP system controls such connectivity. E.g. the PDU session or PDN connecting may be established initially enabling only user traffic between the UAV and the USS/UTM/UFES, and connectivity with the UAV controller is enabled only after the pairing is authorized by the USS/UTM, with appropriate traffic filters installed.

 The authorization of UAV and UAV controller pairing is performed for the purpose of matching a UAV controller with a UAV. During this procedure, the UAV can provide the ID of UAV controller to which it is to be paired, or the UAV controller can provide the ID of the UAV to which it is to be paired. As a result of the authorized pairing, the USS/UTM provides to the 5GS with the authorized UAV and UAV controller pairing information according to the solutions defined in 6.5.3.1 and 6.5.3.2) in case of successful authorization, or information that indicates the authorization of UAV and UAV controller pairing has failed.

If the pairing authorization is successful, the UAV or UAV-C may establish a dedicated UP connectivity for C2 communication between the UAV and the UAV-C, or if there is the existing UP connectivity for communication with the UTM/USS, the network may enable the existing connectivity for C2 communication between the UAV and the UAV-C.

If the pairing authorization fails, the UAV or the UAV-C is not allowed to establish UP connectivity for C2 communication. If there is the existing UP connectivity for communication with the UTM/USS, the UAV or UAV-C may continue to use the connectivity for communication with the UTM/USS only.

 A UAV controller may be controlling multiple UAVs (e.g., swarm/fleet for delivery). In that case, the UAV controller is asummed to perform authorization of pairing with each UAV it wants to control.

5. Flight path authorization/registration for flight operation: the result of this operation is that the USS/UTM verifies all flight related information provided by the UAV, and the USS/UTM may interact with the 3GPP system to e.g. request the UAV location or subscribe to UAV location reporting. During this operation, the USS/UTM can interact with CN to provide information via SCEF/NEF.

Building block 1 is executed in the same way for EPS and 5GS. Building block 2 is executed using existing EPS or 5GS mechanisms.

An External Identifier is allocated as 3GPP UAV ID for the UAV operations. The USS/UTM uses the External Identifier to identify the UAV when requesting services from the 3GPP system.

In one option, the 3GPP UAV ID is a GPSI assigned by the MNO and provisioned as part of the subscription information.In that case, 3GPP UAV ID can be used in UUAA procedure similarly to how GPSI is used in the NSSAA procedure.

#### 6.5.2.3 Applicability to 5GS

For 5GS:

- The procedure for UUAA is performed during the Registration Procedure and is similar to the NSSAA procedure. Following a Registration Procedure with a successful primary authentication, the AMF determines the subscription is for an UAV and indicates to the UAV that there is pending UUAA. The CN then triggers the UUAA with the USS/UTM. UUAA uses credentials obtained by the UAV during registration with the CAA and/or the USS, and include the CAA-Level UAV ID assigned to the UAV during such registration.

- Authorization of UAV and UAV controller pairing and flight path authorization/registration for flight operation: these may take place during PDU Session Establishment for UAV3/UAV5 connectivity and may be based on PDU Session authentication and authorization mechanism already defined for PDU Session Establishment. The UAV uses the same credentials provided in the UUAA.

- an External Identifier is allocated as 3GPP UAV ID for the UAV operations. Such External Identifier in 5GS does not need to be allocated by the USS/UTM and does not need to be known to the USS/UTM via any agreement between the USS/UTM and the 3GPP operator. The External Identifier is provided to the USS/UTM by the 3GPP system during the procedures described in this solution.

#### 6.5.2.4 Applicability to EPC

For EPC:

- a dedicated APN is used for UAVs connectivity to USS and to support UAV3/UAV5 connectivity. Connectivity for aerial traffic is not allowed over other PDN connections

- an External Identifier is allocated as 3GPP UAV ID for the UAV operations. In EPC, it is assumed that the PDN GW is configured with pre-defined PCC rules which enable the PDN GW to provide additional information with header enrichments, and convey at least the External Identifier.

- UUAA, Authorization of UAV and UAV controller pairing, and Flight path authorization/registration for flight operation, when performed, take place during PDN Connection Establishment. Establishment of such PDN Connection is always authorized for a UAV with aerial subscription, using PCO-based mechanisms and NAS transport.

- The authorization is performed between the UAV and the USS/UTM as in the 5GS case. If the authorization fails, the PDN connection is not established, and the network may keep the device registered in the 3GPP system or deregister it based on the network policy. If the network keeps it registered, the network should disable the UAV related functionalities for the device.

- Authorization of UAV and UAV controller pairing and Flight path authorization/registration for flight operation are also performed between the UAV and the USS/UTM via PCO communications.

- PCO is extended to enable the UE to carry the information for UUAA, Authorization of UAV and UAV controller pairing, and Flight path authorization/registration for flight operation between the UAV and the UAV controller.

Editor's note: Whether an application-level solution is considered in the EPC case is FFS. In such solution, the UE interacts via user plane over a PDN connection with an Application Server that verifies the validity of the UUAA and Flight path authorization/registration for flight operation, and informs the EPS via SCEF of the success/failure of the procedures. Until the procedure succeeds, the UAV can only connect with such server. The USS may act as such server.

In the EPC scenario, two options may be considered:

- a new PDN connection establishment takes place at each pairing/flight authorization; or

- a default PDN connection with default bearer for UAV-USS traffic is established at attach (such bearer enables only communication between the UAV and the USS), and dedicated bearers are established for C2 between the UAV and the UAV controller and triggered by USS acting as SCS/AS towards the UFES which acts as a SCEF.

Though the solution suggests the use of default APN and DNN for UAV services, the solution does not advocate but does not oppose the use of specific well-known APN/DNN for UAV services. The solution addresses both UAVs that are UE using only UAV services, and UAVs that may support other type of data network connectivity for other services.

### 6.5.3 Procedures

#### 6.5.3.1 5GS Procedure

The procedure for UAV Authentication and Authorization by USS in the 5GS case is depicted in Figure 6.5.3-1.



Figure 6.5.3-1: Procedure for UAV Authentication and Authorization with USS/UTM in 5GS

1. [Outside the scope of 3GPP] A registration is performed for the UAV by the UAS operator. The USS is informed of the UAV being registered (procedure out of scope of 3GPP, details defined outside 3GPP). UAS operator provides UAV's aviation-level information, e.g. UAV identification (serial number of the UAV), Pilot information, UAS make and model number, etc. Details may change depending on the USS and CAA. UAV is assigned a CAA-level UAV ID. The procedure can be carried out over 3GPP user plane connectivity.

NOTE 1: It is assumed that the CAA-level UAV ID can be resolved to an address of the USS serving the UAV (e.g. DNS lookup, or other resolution mechanisms defined outside 3GPP, as in the case of the ASTM standard).

2. [Outside the scope of 3GPP] [Optional] UAS operator request a flight path authorization/registration for flight for a UAV with USS (procedure is out of scope of 3GPP). UAS operator provides CAA-level UAV ID and e.g. flight Information, altitude, time of flight. Details change depending on USS and CAA. UTM/USS optionally assigned a Flight Authorisation ID for the authorised flight. The format of the Flight Authorization ID is defined outside 3GPP. This step may be performed offline or via 3GPP user plane connectivity. The request for flight path authorization may be also carried out in step 8 (Authorisation for UAV operation - Option 1) or step 12 (Authorisation for UAV operation - Option 2).

NOTE  2: It is assumed that the Flight Authorization ID contains information that can be resolved to an address of the USS serving the UAV (e.g. DNS lookup, or other resolution mechanisms defined outside 3GPP, as in the case of the ASTM standard).

3. The UE triggers a Registration Request procedure.The UE indicates support for UUAA/UAS operations capabilities. The UE includes a UAV identity (e.g. a permanent identity) to indicate that it wishes to register for the UAS service. The UE may omit such indication if it wishes to perform a Registration as a regular UE (i.e., not using UAS service, performing UUAA etc).

NOTE 3: It is assumed that the UE may trigger a UAV authentication and authorization by means of a mobility or initial registration procedure.

4. The network performs a primary authentication during the Registration Procedure as specified in TS 23.501 [12] clause 4.2.2.2.2.

5. The AMF determine whether a USS UAV Authorization/Authentication (UUAA) is required based on the UAV subscription and UE capabilities.

NOTE 4: It is assumed that in 5GS the subscription is marked as an aerial subscription, as already enabled in EPC since Rel. 15.

6. [Optional, if UUAA is performed] The AMF returns a Registration Accept message to the UAV containing a "pending UUAA" indication if the UUAA needs to be performed. The AMF assigns the Tracking Areas of the Registration Area as a Non-Allowed Area (i.e. the UAV is only allowed to exchange NAS signalling and is not allowed to trigger a PDU session establishment, among other procedures). The AMF may return also other configuration information, e.g. UAS information such as types of communication allowed by the operator for UAS operations (e.g. network-assisted, direct, etc.). Upon receiving the "pending UUAA" indication the UAV behaves as a UE receiving a "Pending NSSAA" indication and is restricted from performing e.g. any PDU session establishment dedicated for the UAS service.The UE may access any other non-UAS PDU sessions (e.g., for software update). Such PDU sessions may be have been established prior to the UUAA (e.g., when UUAA is triggered by a Mobility Registration procedure) or after.

7. [Optional UUAA, not performed if 8 is performed] The AMF triggers a UUAA procedure. The UAV in the UUAA uses credentials obtained by the UAV during registration with the CAA and/or the USS, and include the CAA-Level UAV ID assigned to the UAV during such registration. The UAV may include an UUAA Aviation Payload containing application layer information that is transparent to the AMF.

 The UAV GPSI may be provided by the AMF to USS if procedure is directly between AMF and USS. PEI may be provided to USS by the AMF. USS stores GPSI.

 Upon successful UUAA, the AMF receives UAV authorization information from USS/UTM during the procedure.

 The AMF (or the UFES, details TBD) provides the External Identifier of the UAV to the USS.

NOTE 5: The details of UUAA procedure depends on the security model (i.e. security credentials) used at the application level to secure the communications between the UAV and the USS and to secure the Remote Identification solution. It is assumed that such security mechanisms, similarly to V2X, are defined at the application layer and outside a 3GPP. The UUSS may e.g. be based on EAP authentication between the UAV and the USS via the AMF, in which case the UUAA procedure is similar to the NSSAA procedure.

NOTE 6: The UUAA procedure is executed over NAS Transport, and in the case of the NSSAA procedure.

The AMF provides the UAV GPSI to the UFES which acts as a proxy towards USS/UTM, similar to NSSAAF in a NSSAA procedure.

8. [Optional, not performed if 7 is performed] This option proposes combined authorization for pairing UAV controller and UAV and for UAV flight authorization by the UTM/USS in addition to UUAA. This is considered Option 1 for authorization for pairing UAV controller and UAV and for UAV flight authorization by the UTM/USS. The same function of step 7 is performed, but in this option the UAV includes in the UUAA Aviation Payload also the information for the authorization of UAV and UAV controller pairing, e.g. the ID of the UAV controller with which the UAV expects to match or the ID of UAVs for which the UAV controller expects to control, and the information for flight path authorization/registration for flight operation, thus all three types of authorization are performed jointly.

 Upon successful UUAA, the AMF receives UAV authorization response information from USS/UTM during the procedure which may include the authorized UAV and UAV controller pairing information, e.g., the ID of the UAV controller with which the UAV allows to match or the ID of UAVs for which the UAV controller allows to control.

The AMF stores the UAV authorization information to determine later wether to allow UE to establish a PDU session dedicated for the UAS service. Such information may include an authorized CAA-level UAV ID assigned by the USS/UTM. A networked UAV controller may be paired with more than one UAV and therefore be provided with more than one authorized CAA-level UAV ID.

 Upon unsuccessful UUAA, the AMF receives UAV authorization response information which may indicate that the authorization of UAV and UAV controller pairing is failed.

9. Upon successful UUAA, the AMF triggers the UE Configuration Update procedure to deliver a new Registration Area. The AMF may deliver additional information if received from UFES/USS (e.g. a new CAA-level UAV ID).

10. The UE sends a PDU Session Establishment Request message to the SMF in order to establish a C2 connection with a UAV controller and connection with the USS/UTM.

 The UAV provides a "UAV operation request indication", which may be an explicit indication, or a specific DNN, or a specific combination of DNN and S-NSSAI, to indicate to the SMF that the PDU Session is for communication with USS and for C2. The indication may include the authorized CAA-level UAV ID assigned by the USS/UTM received following a successful UUAA. When paired with more than one UAV, a networked UAV controller may select and include a particular CAA-level UAV ID in the request.

Editor's note: Whether an explicit indication, a dedicated DNN, or a combination of dedicated DNN and S-NSSAI is used is FFS.

NOTE 7: A dedicated well-known DNN may be used for UAV services, but this should be defined outside 3GPP (e.g. in GSMA) for roaming and interworking purposes. At a minimum, the UAV needs to be configured with the DNN to be used for UAV services or the MNO needs to set the Default DNN to correspond to the APN for UAV services.

 Option 2 for authorization for pairing UAV controller and UAV and for UAV flight authorization by the UTM/USS supports authorization for establishment of a PDU session for UAV operations by the UTM/USS. In this option the UAV has already been authenticated by the UTM/USS in previous steps. The UAV provides to the SMF with an Aviation Connectivity Payload containing the CAA-Level UAV ID, and the Flight Authorisation ID if the UE obtained one at step 2. If the UAV did not perform step 8 and the option in step 12 is used, the UAV includes also the information for flight path authorization/registration for flight operation. If the UAV did not perform step 2 or the information has changed, the UAV includes also the information for the authorization of UAV and UAV controller pairing as in step 8.

Editor's note: The container provided by the UE may be transparent to the SMF and provided directly to the USS/UTM, or may contain some parameters that the SMF verifies or augments (e.g. UAV location) based on the UAV subscription before triggering the authentication/authorization towards the USS/UTM.

Editor's note: Depending on the exact format of the CAA-Level UAV ID the UE may not need to include this identifier in the PDU Session Establishment request.

11. The SMF retrieves the SM subscription data from UDM. The SMF may select a USS (e.g. based on subscription data), or may delegate the selection to the UFES.

NOTE 8: It is assumed that it is possible for the UAV subscription to contain the USS information, e.g. for scenarios of tight coupling between the MNO and the USS in which case the USS information can be stored in the UAV subscription data.

12. [Optional, alternative to step 13]

12a. The SMF sends an UAV Operation Request (e.g. using a service interface) to the UFES, including the CAA-level ID, Flight Authorisation ID, UAV Location, GPSI, and optionally USS information determined in step 11. The SMF may also include the PEI.

12b. If the SMF does not include the USS information, the UFES selects a USS based on subscription data or CAA-level UAV ID and/or Flight Authorization ID.

12c. The UFES forwards the information to the USS.

12d. The USS validates the request based on the CAA-Level UAV ID, the PEI, and the Flight Authorization ID (if one is provided).

 The USS determine Remote Identification & Tracking Info (RITI) for the UAV to use. This may include a new CAA-level UAV ID (e.g. a temporary identity for Remote Identification) that is used as a means to remotely identify the UAV, and Authorisation Data that may include the authorised area & time where the UAV can operate, UAV type. The USS also determines Authorization Data containing information about the user plane connectivity between the UAV and the UAV Controller. Some of the RITI information, e.g. the CAA-level UAV ID, are received and stored by the UFES, together with the Authorization Data.

Editor's note: Whether additional RITI information is processed by the 3GPP system is FFS.

12e. The USS sends a UAV Operation Accept to the UFES containing the Authorization Data and RITI. The Authorization data may include the authorized UAV and UAV controller pairing information, e.g. including the ID of the UAV controller with which the UAV allows to match or the ID of UAV for which the UAV controller allows to control.

12f. The UFES sends a UAV Operation Accept to the USS containing the Authorization Data and RITI. The UFES may store the correspondence between the CAA-Level UAV ID, the 3GPP UAV ID, the Authorization Data, and the RITI.

13. [Optional, alternative option 1 and to option 2 defined in steps 10-12] This option relies on the signaling support for secondary PDU session authentication to authorize the pairing of UAV controller and UAV and for UAV flight authorization by the UTM/USS. The SMF trigger the secondary authorization/authentication of the PDU session during the PDU Session establishment. The information exchanged between UAV and USS/UTM for authorization for pairing UAV controller and UAV can refer to step 8.

Editor's note: The information provided by the UE may be transparent to the SMF and provided directly to the USS/UTM, or may contain some parameters that the SMF verifies/augments (e.g. location) based on the UAV subscription before triggering the authentication/authorization towards the USS/UTM.

Editor's note: Whether an actual authentication takes place depends on the security solutions defined for the communication between the UAV and the USS.

14. The SMF configure user plane connectivity for UAV to UAV Controller communication based on information that the USS may provide (e.g. policies and/or traffic filters) to enable user plane connectivity between the UAV and the UAV controller.

NOTE 9: This may be performed via PCF if the USS acts as an AF and provides connectivity policies via PCF, or via the UFES.

15. The PDU session establishment succeeds only upon indication from the USS that either step 12 or 13 succeeded. The SMF forwards the RITI to the UAV within the PCO of the session management message.

Editor's note: The details of the exchange of aviation level information such as RITI in NAS signaling (e.g. PCO or new IEs) are FFS.

16. UAV broadcasts remote identification information for remote identification based on RITI information.

17. UAV sends remote identification information to the USS based on RITI information.

18. The UE exchanges C2 traffic with the UAV Controller.

#### 6.5.3.2 EPS Procedure

The procedure for UAV Authentication and Authorization by USS in the EPS case is depicted in Figure 6.5.3-2.



Figure 6.5.3-2: Procedure for UAV Authentication and Authorization with USS/UTM in EPS.

1. [Outside the scope of 3GPP] A registration is performed for the UAV by the UAS operator. The USS is informed of the UAV being registered (procedure out of scope of 3GPP, details defined outside 3GPP). Details may change depending on the USS and CAA. UAV is assigned a CAA-level UAV ID. The procedure can be carried out over 3GPP user plane connectivity.

NOTE 1: It is assumed that the UAV and/or the CAA-level ID can be resolved to an address of the USS serving the UAV (e.g. DNS lookup, or other resolution mechanisms defined outside 3GPP, as in the case of the ASTM standard).

2. [Outside the scope of 3GPP] [Optional] UAS operator requests a flight path authorization/registration for flight for a UAV with USS (procedure is out of scope of 3GPP). UAS operator provides CAA-level UAV ID and e.g. flight Information, altitude, time of flight. Details change depending on USS and CAA. UTM/USS optionally assigned a Flight Authorization ID for the authorized flight. The format of the Flight Authorization ID is defined outside 3GPP. This step may be performed offline or via 3GPP user plane connectivity. The request for flight path authorization may be also carried out in step 3 via PCO.

NOTE 2: It is assumed that the Flight Authorization ID contains information that can be resolved to an address of the USS serving the UAV (e.g. DNS lookup, or other resolution mechanisms defined outside 3GPP, as in the case of the ASTM standard).

3. The UAV sends an Attach Request to the MME. In EPS, Protocol Configuration Options (PCO) in the ESM message container are used to transfer parameters between the UE and the PDN GW, and sent transparently through the MME and the Serving GW. The PCO is extended to enable the UAV to insert the CAA-Level UAV ID, the Flight Authorization ID (if available), and the Aviation Connectivity Payload containing the information for flight path authorization/registration for flight operation and for the authorization of UAV and UAV controller pairing (the information exchanged between UAV and USS/UTM for authorization for pairing UAV controller and UAV can refer to clause 6.5.3.1).

Editor's note: Depending on the exact format of the CAA-Level UAV ID the UE may not need to include this identifier in PCO in the ESM message container.

4. Primary authentication/authorization is performed as specified in TS 23.401 [10] clause 5.3.2.1.

5. The MME determines the UAV has an aerial subscription and selects the Default APN for connectivity with the USS.

6. The MME sends a Create Session Request to the PGW via the SGW. The MME may include the ME Identity (IMEISV of the UAV). The MME selects a PDN GW suitable to serving the Default APN, which must resolve to a PGW that can interface with the UFES (this may be e.g. for Radius operations if Radius is used between the PGW and the UFES). For the default APN used for connectivity with the USS, the HSS must allow selection of a PDN GW in the VPLMN for the Default APN.

NOTE 3: A dedicated well-known APN may be used for UAV services, but this should be defined outside 3GPP (e.g. in GSMA) for roaming and interworking purposes. At a minimum, the UAV needs to be configured with the APN to be used for UAV services or the MNO needs to set the Default APN to correspond to the APN for UAV services.

7. The UUAA, authorization of UAV and UAV controller pairing, and flight path authorization/registration for flight are performed.

7a. The PGW provides the information sent by the UAV in the PCO (CAA-level UAV ID, Flight Authorization ID, Aviation Connectivity Payload) and the UAV's IMEISV (if provided) to the UFES. The PDN GW is configured with pre-defined PCC rules which enable the PDN GW to provide additional information with header enrichments, and convey at least the External Identifier.

Editor's note: Whether Radius can be re-used for the interface between the PGW and the UFES is FFS.

7b. The UFES selects the USS based on the information received from the UAV (e.g. the CAA-level UAV ID and/or Flight Authorization ID).

7.c. The UFES forwards the information to the USS.

7.d. The USS validates the request based on the CAA-Level UAV ID, the Flight Authorization ID (if one is provided).

 The USS determine Remote Identification & Tracking Info (RITI) for the UAV to use. This may include amongst others, a new CAA-level UAV ID, a UAV Type that is used as a means to remotely identify the UAV. The USS also determines Authorization Data containing information about the user plane connectivity between the UAV and the UAV Controller, and for connectivity between the UAV and the USS. Some of the RITI information, e.g. the CAA-level UAV ID, are received and stored by the UFES, together with the Authorization Data.

Editor's note: Whether additional RITI information is processed by the 3GPP system is FFS.

7.e. The USS returns the response to the UFES.

7.f. The UFES returns the response to the PGW.

8. [Optional] if the PGW received the Authorization Data (including authorized UAV and UAV controller pairing information), the PGW installs traffic filters for the connectivity between the UAV and the UAV controller, and for connectivity between the UAV and the USS.

9. The PGW confirms the procedure to the MME along with providing the RITI in the PCO.

10. The new MME sends an Attach Accept to the UE with the PCO containing the RITI.

11. [Optional] After step 7, the USS acts as an SCS/AS and communicates to the UFES, which acts as a SCEF, to trigger the establishment of an application session with a required QoS and providing traffic filters to enable UAV to UAV controller connectivity, and optionally for UAV to USS connectivity. The USS may also use other SCEF services of the UFES.

12. UAV broadcasts remote identification information for remote identification based on RITI information.

13. UAV sends remote identification information to the USS based on RITI information.

14. The UE exchanges C2 traffic with the UAV Controller.

### 6.5.4 Impacts on services, entities and interfaces

Editor's note: This clause describes impacts to services, entities and interfaces.

For 5GS:

- The AMF is enhanced to provide the "UUAA pending" indication to the UAV.

- The SMF supporting the DNN or DNN+S-NSSAI combination used for UAV connectivity to USS and UAV-UAV controller connectivity are enhanced to exchange direct signalling to the USS via the UMF (option of step 12), otherwise it relies on an EAP mechanism (TBD) for secondary PDU session authentication and authorization.

For EPS:

- The PDN GW interfaces with the UFES for the UAV APN.

Editor's note: The exact details of the interface are FFS.

For both EPS and 5GS:

- An UFES function is introduced as described above. The UFES may be mapped to existing functionality, e.g. SCEF, NEF, AAA-P depending on the specific implementation of the interfaces between the 3GPP system and the USS/UTM.

**\* \* \* \* End of Change \* \* \* \***