**3GPP TSG-WG SA2 Meeting #145E e-meeting *S2-210xxxx***

**Elbonia, May 17– 28, 2021 (revision of S2-210xxxx)**

**Source: Huawei, HiSilicon**

**Title:** **Clarification on terms related to UAV communication**

**Document for: Approval**

**Agenda Item: 8.7**

**Work Item / Release:** **ID\_UAS / Rel-17**

*Abstract:* *This contribution proposes to clarify the terms related to UAV communication.*

# 1. Introduction/Discussion

The term "UAV communication" appears several times in the current specification but we have never define it. When we looked at the specification carefully, we found confusion in the use of terms related to UAV communication and unclear concepts. Thus it is proposed to remove the term "UAV communication" and define a new term "USS communication".

The USS communication is between UAV and USS, and for UAS services other than C2 communication. The communication for UAS services consist of C2 communication and USS communication. UUAA-SM is performed during session management procedures for USS communication and C2 authorization is performed during session management procedures for C2 communication.

# 2. Text Proposal

It is proposed to capture the following changes vs. TS 23.256.

\* \* \* \* First change \* \* \* \*

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.
A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1] or TS 23.501 [2].

**3GPP UAV ID:** Identifier assigned by the 3GPP system and used by external AF (e.g. USS) to identify the UAV. GPSI is used as the 3GPP UAV ID.

**Broadcast Remote ID:** The capability of providing Remote Identification and Tracking over broadcast radio links.

NOTE: In the scope of this release, the radio link for Broadcast Remote ID is assumed to utilize radio technologies outside the scope of 3GPP.

**CAA (Civil Aviation Administration)-Level UAV Identity:** a UAV identity assigned by USS/UTM, and uniquely identifies a UAV at least within the scope of a USS.

**Command and Control (C2) Communication:** the user plane link to deliver messages with information of command and control for UAV operation from a UAV controller or a UTM to a UAV or to report telemetry data from a UAV to its UAV controller or a UTM.

**Networked UAV Controller:** a UAV Controller connected to the 3GPP network and connected to the UAV via a 3GPP network.

**Non-Networked UAV Controller:** a UAV Controller not connected to the 3GPP network and connected to UAV via a transport outside the scope of 3GPP, e.g. internet connectivity or direct wireless communication over a technology outside the scope of 3GPP.

**Networked Remote ID:** The capability of providing Remote Identification and Tracking to a USS over 3GPP network.

**Remote Identification (Remote ID) of UAS:** The ability of a UAS in flight to provide identification and tracking information that can be received by other parties, to facilitate advanced operations for the UAS (such as Beyond Visual Line of Sight operations as well as operations over people), assist regulatory agencies, air traffic management agencies, law enforcement, and security agencies when a UAS appears to be flying in an unsafe manner or where the UAS is not allowed to fly. The Remote ID information payload may include Serial Number or Session ID assigned to the UAV, location of the ground-station controller, emergency status indication, etc.

**Third Party Authorized Entity:** is either a privileged Networked UAV Controller, or a privileged Non-Networked UAV Controller, or another entity which gets information on sets of UAV controllers and UAVs from the 3GPP network, and may be connected to the UAV via the Internet; it may be authorized by the UTM to interface with sets of UAV(s).

**UAS NF:** a 3GPP UAS Network Function for support of aerial functionality related to UAV identification, authentication/authorization and tracking, and to support Remote Identification.

**UAS Service Supplier (USS):** An entity that provides services to support the safe and efficient use of airspace by providing services to the operator / pilot of a UAS in meeting UTM operational requirements. A USS can provide any subset of functionality to meet the provider's business objectives (e.g. UTM, Remote Identification). In the scope of this specification, the term USS refers to both USS and USS/UTM.

**UAS Traffic Management (UTM):** a system that can safely and efficiently integrate the flying UAV along with other airspace users. It provides a set of functions and services for managing a range of autonomous vehicle operations (e.g. authenticating UAV, authorizing UAS services, managing UAS policies, and controlling UAV traffics in the airspace).

**UAV controller:** The UAV controller of a UAS enables a drone pilot to control an UAV.

**UAV operator:** the entity owning and operating a UAV.

**UAS Services:** refers to establishment of connectivity for a UAS for communication with USS, for C2, for remote identification, and for UAV location and tracking.

**USS communication:** the user plane data for UAS Services other than C2 communication between UAV and USS, e.g. for remote identification, UAV location and tracking, etc.

**UUAA Autorization Payload**: Contains application layer information exchanged between the UAS and the USS and that is transparent to the 3GPP System.

**UUAA Aviation Payload:** Contains application layer information exchanged between the UAS and the USS and that is transparent to the 3GPP System

**Uncrewed Aerial System (UAS):** Composed of Uncrewed Aerial Vehicle (UAV) and related functionality, including command and control (C2) links between the UAV and the control station, the UAV and the network, and for remote identification. An UAS may comprise of a UAV and a UAV controller.

**Unknown UAVs**: A list of the UAVs to be identified in the target area and served by the PLMN as the result of the UAV tracking requested by USS/UTM.

**UUAA:** UAV USS authentication and authorization procedure of the UAV to ensure that the UAV has successfully registered with a USS and has therefore been authorized for operations by the USS. An UAV is authenticated and authorized by USS via a UUAA procedure with the support of the 3GPP system before connectivity for UAS services is enabled.

**UUAA-MM:** the UUAA procedure optionally performed during registration to a 5GS.

**UUAA-SM:** the UUAA procedure optionally performed (when UUAA-MM is not performed) during the establishment of a PDU session for USS communication, and performed during the establishment of a PDN connection for USS communication.

\* \* \* \* Second change \* \* \* \*

### 4.2.1 General

This specification covers UAV functionality provided by 5GC connected to NG-RAN and EPC connected to LTE.

The following functionality is defined for UAV support in the 3GPP system:

- An UAV is authenticated and authorized by USS via a USS UAV Authentication & Authorization (UUAA) with the support of the 3GPP system before connectivity for UAS services is enabled.

- Depending on 3GPP network operator and/or regulatory requirements, the UUAA is performed:

- In 5GS: either as a separate procedure during the 5GS registration procedure (optional and based on specific PLMN policies, USS requirements, and geographic regulatory requirements), or when the UAV requests user plane resources for UAV operation (i.e. PDU session establishment). The UAV shall support UUAA during Registration and PDU session establishment procedure. The network shall support UUAA during PDU session establishment.

- In EPS: during the attach procedure and the corresponding PDN connection establishment. The network shall support UUAA during PDN connection establishment. The UAV shall support UUAA during PDN connection establishment procedure.

- A UAV that is in possession of a CAA-Level UAV ID provides the CAA-Level UAV ID in 5GS in both Registration and in PDU Session establishment. In EPC, a UAV that is in possession of a CAA-Level UAV ID provides the CAA-Level UAV ID in PDN Connection establishment in SM-PCO. The CN determine whether UUAA is executed at 5GS registration or at PDU session/PDN Connection establishment, based on local policies.

- If UUAA is not performed during the Registration procedure in 5GS, the UUAA is performed at PDU session establishment when the UAV requests user plane resources for UAV operation and the UAV provides its CAA Level ID during PDU session (PDN connection) establishment.

- The UAV flight authorization and UAV-UAVC pairing authorization is performed at PDU session/PDN connection establishment/modification procedures.

- The 3GPP system supports USS authorization of pairing between a UAV and a networked UAVC or a UAVC that connects to the UAV via Internet connectivity during the establishment of the PDN connection/PDU session for C2 communication. Modifications or establishment of the pairing or re-authorization take place via modification of the established PDN connection/PDU session. During such procedures, the USS provides to the 3GPP system information (e.g. QoS requirement, data flow descriptors, etc.) that enable traffic between the UAV and the UAVC.

NOTE: How the USS is made aware of the UAVC is outside the scope of 3GPP in this Release.

- For EPC, the PDN connections used by UAV are served by SMF+PGW-C regardless of whether the UAV support 5G NAS or whether their subscription allows access to 5GC. The APN(s) used by the UAV for contacting USS or for C2 communication always resolves to a SMF+PWG-C.

The following architectural assumptions apply:

- It is assumed that the UAV trying to access UAS services using 3GPP connectivity is already registered with a USS and has been assigned a CAA-Level-UAV ID. The procedure for UAV registration and assignment of CAA-Level-UAV ID is out of scope of 3GPP. The USS assigns to the UAV a CAA-Level UAV ID, or is made aware of the assigned CAA-Level UAV ID.

- A UAV is associated with an Aerial subscription in the UDM. The Aerial subscription contains aerial UE indication (to be used similarly to aerial UE indication defined in EPS) and SM data that indicate that authentication/authorization has to be done using API based mechanism, and optionally some information to determine the dedicated NF (e.g. UAS NF) to contact for authentication and authorization.

- An UAV is identified by USS using a CAA-level UAV ID, and identified by the 3GPP System using a 3GPP UAV ID assigned by the MNO:

- It is assumed that an aerial subscription associated to a UAV includes at least one GPSI to be used as 3GPP UAV ID.

- A UAV is registered with the USS either before connecting with the 3GPP system or using plain internet connectivity via the 3GPP system. Before registering for UAS services with the 3GPP system, the UAV shall be provisioned with a CAA-Level UAV Identity.

- In roaming scenarios, it is assumed that access to USS is in the VPLMN, thus packet data connectivity for UAV-USS communication is in local breakout, and the UAS NF function is located in the VPLMN.

- In this Release, the UAV uses 3GPP access (i.e. LTE & NR) for 3GPP UAV related operations.

- Activation of RAN aerial features for UAV accessing via E-UTRA reuses the existing mechanism defined in TS 36.300 [7].

- For this Release, it is assumed a UAV is served by the same USS for the duration of a flight.

- One or more USS(s) may be present in a specific region and may manage UAVs over one or more 3GPP networks.

- The 3GPP Network subscription for the UAV is not assumed to contain any information about the USS.

- The USS address, if known to the UAV, is configured in the UAV via mechanisms outside the scope of 3GPP.

\* \* \* \* Third change \* \* \* \*

### 4.3.5 SMF

In addition to the functionality defined in TS 23.501 [2], the SMF:

- triggers the UUAA-SM procedure for a UE requiring UAV authentication and authorization by a USS when requesting user plane resources for UAV operation, or when the USS/UTM that authenticated the UAV triggers a re-authentication;

- may trigger the authorization of pairing between a UAV and a networked UAVC or a UAVC that connects to the UAV via Internet connectivity during the establishment of the PDN connection/PDU session for C2 communication.

\* \* \* \* Fourth change \* \* \* \*

### 5.2.1 UUAA Model

The following applies for UUAA for a UAV:

- UUAA-MM is optional and performed at 5GS registration based on operator’s policy. If required by the operator, UUAA-MM is performed if the UAV has an aerial UE subscription in the Access and Mobility Subscription Data and provides the CAA-Level UAV ID in the Registration Request message. If UUAA-MM is not performed, the UAV shall be authenticated at PDU session establishment in UUAA-SM.

- UUAA-SM is required at each PDU session establishment (PDN connection in EPS) for USS communication. The UUAA-SM is triggered by the SMF (SMF+PGW-C in EPS) based on the SM subscription data and the UAV provides the CAA-Level UAV ID in the PDU Session Establishment Request message in case of 5GS, or in the ESM message container in case of EPS.

- UUAA-SM is performed at each PDU session modification or EPS bearer modification (e.g. in case of C2 authorization or flight plan authorization change) if the UE includes CAA-Level UAV ID and a UUAA Aviation Payload.

Editor’s Note: How to prevent UAV uses the UAS service without providing the CAA-Level UAV ID and a UUAA Aviation Payload is FFS.

\* \* \* \* Fifth change \* \* \* \*

#### 5.2.2.2 UUAA-MM Procedure



Figure 5.2.2.2-1: UUAA-MM procedure

1. For a UE that requires UUAA or when triggered by re-authentication by USS, the AMF triggers a UUAA-MM procedure.

2. AMF to UAS NF: The AMF invokes Nnef\_Auth\_Req service operation that shall include the GPSI and the CAA-Level UAV ID and may include USS address (e.g. FQDN). UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address, as described in clause 4.4.2.

NOTE 2: Security details will be determined by SA WG3.

Editor's note: Whether and how the USS address is protected by the UAV is FFS.

3. UAS NF to USS: Authentication Request, shall include the GPSI and CAA-Level UAV ID.

4. [Conditional] Multiple round-trip messages as required by the authentication method used by USS. Authentication Response messages from USS shall include GPSI and may include a authentication message based on authentication method used that is forwarded transparently to UE over NAS MM transport messages. The Authentication Response message from USS in step 4a may also contain a callback URI to be used by the UAS NF for subsequent authentication request in step 4f.

5. USS to UAS NF: (final) Authentication Response, shall include: GPSI, a UUAA result (success/failure), may include an authorized CAA-level UAV ID and a payload delivering configuration information to the UAV (e.g. security info to be used to secure communications with USS), and a final authentication message (e.g. indicating success or failure) based on authentication method used that is forwarded transparently to UE over NAS MM transport messages.

6. UAS NF to AMF: (final) Authentication Response, forwards information received from USS in step 5.

7. AMF to UE: (final) NAS MM transport message forwarding authentication message from USS including authentication/authorization result (success/failure).

8. [Conditional] if UUAA-MM succeeded, AMF triggers a UE Configuration Update procedure to deliver to the UAV authorization information from USS, as described in clause 5.2.2.1. If UUAA-MM fails during a Re-authentication and Re-authorization and there are PDU session(s) established for C2 communication, AMF triggers these PDU Sessions release with the appropriate cause value. AMF identifies which PDU session is for C2 communication based on the DNN/S-NSSAI value of the PDU session.

9. [Conditional] if UUAA-MM fails, based on network policy the AMF may trigger Network-initiated Deregistration procedure described (as specified in TS 23.502 [3], clause 4.2.2.3.3) and it shall include in the explicit De-Registration Request the appropriate rejection cause value.

At any time after the initial registration, the USS (via UAS NF) or the AMF may initiate Re-authentication procedure for the UAV. For AMF initiated case the Re-authentication procedure shall start from step 2. USS initiated re-authentication procedure is described in clause 5.2.4.

Editor's Note: It is FFS how the UAS NF is informed of a new serving AMF when the UUAA context is transferred to a new AMF.

\* \* \* \* Sixth change \* \* \* \*

#### 5.2.3.1 General

Editor’s Note: This procedure will be revisited after security aspects on UUAA are determined by SA3.

An UAV uses PDU Sessions or PDN Connections for connectivity with the USS and for connectivity with a networked UAV-C.

A networked UAV-C is a UE which uses existing procedures for establishing PDU Session or PDN Connection for communication with the USS/UTM, and the procedures described in this clause do not apply to a networked UAV-C.

This clause describes procedure that applies both for 5GS and EPS, where PDU Session refers to 5GS and PDN Connection refers to EPS.

PDU Session(s)/PDN Connection(s) for UAS services shall only be established after a UAV has been authenticated and authorized by the USS this may happen during UUAA-MM, as described in clause 5.2.2, , or during UUAA-SM as described in this clause.

A UAV may use either a common or separate PDU Session/PDN connection for connectivity with the USS and a UAV-C.

When the UAV requests establishment of a PDU session/PDN connection, the PDU session/PDN Connection may require UUAA authorization, subject to operator, regulatory requirements as described in clause 5.2.4.

If the UAV uses the PDU session/PDN connection for C2 the PDU session is subject to C2 authorization as described in clause 5.2.5.

The UAV shall indicate that the PDU Session/PDN Connection is for the USS communication and/or C2 communication in the PDU Session Establishment/PDN Connectivity request. The PDU Session/PDN Connection is identified by the SMF/SMF+PGW-C as being for USS/C2 communication based on the DNN or DNN/S-NSSAI combination.

During the establishment or modification procedure of the PDU Session/PDN connection for C2 communication, the USS shall provide the 3GPP system with following information for enabling basic C2 communication between UAV and UAV-C:

- traffic filters

- QoS requirements

The USS can enable/disable C2 communication between UAV and UAV-C necessary for services used during the flight operation at any point in time as described in clause 5.2.9.

Clause 5.2.3.2 defines the USS UAV Authorization/Authentication (UUAA) procedures at PDU Session Establishment in 5GS and clause 5.2.3.3 is for the PDN Connection Establishment in the Attach procedure for EPS using the interworking functionality. Editor’s Note: The naming for the procedures and IEs, where needed, will be updated to make them generic (i.e. not specific to ID\_UAS).

When the UAV - UAV-C pairing authorization is revoked by the USS, the SMF or SMF+PGW-C shall release the PDU Session/PDN connection for C2 communication (in case separate PDU Sessions/PDN Connections are used), or disable C2 communication for the PDU Session/PDN connection (in case separate connections are used).

When the UUAA is revoked by the USS, all UAV related PDU Session/PDN connections shall be released.

\* \* \* \* Seventh change \* \* \* \*

##### 5.2.5.2 Procedure for C2 authorization in 5GS

If C2 authorization is requested during the UUAA-SM procedure the procedure described in clause 5.2.3.2 takes place with the following additions:

- In Step 0, the UAV includes a within a UAS container, pairing information (if available)

- In step 5, the SMF may receive authorization information for C2 from the USS. The SMF then interacts with the PCF to retrieve the associated policy rules based on the authorization information provided by the USS to enable the requested C2 communication. The SMF configures the UPF based on the policy rules provided by the PCF to enable the requested C2 communication.

If C2 authorization is requested:

- After UUAA-SM is performed and a common PDU session is used for connectivity to USS and UAV-C or

- If the UAV has already established a PDU session for connectivity to a UAV-C

The UAV requests C2 authorization at PDU session modification as follows:



Figure 5.2.5.2-1: PDU Session modification for C2 communication (common PDU session for UAS services)

1. The UAV establishes a PDU Session for USS communication as described in clause 5.2.3.

2. The UAV requests C2 authorization by initiating PDU Session Modification procedure. The UAV includes the pairing information as part of UAS container in the PDU Session modification request. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization. The pairing information includes the CAA-level UAV ID of the requesting UAV and also includes identification information of UAV-C to pair if available. The UAS container may include other information such as Flight Authorization information.

NOTE: How the pairing information is configured in the UAV is outside the scope of 3GPP specifications.

3. The SMF invokes the authorization procedure with the USS (via UAS-NF) as described in clause 5.2.3. The SMF also includes the UAS container provided by the UAV in step 2. The USS shall inform the SMF, through the UAS-NF as described in clause 5.2.3, the result of the authorization. If the pairing information is included in the authorization request, the authorization request is also used to request authorization to pair the UAV with UAV controller and the authorization response implicitly or explicitly indicates whether the UAV is allowed to be paired with the UAV controller. The USS determines remote identification and tracking information that may also include a new CAA-level UAV ID for the UAV during the pairing authorization procedure and send it together with the authorization result to the SMF. The SMF may receive authorization information for C2 from the USS and continues the PDU session modification procedure. The authorization information includes UAV-C IP address.

Editor's note: How the UAV indicates that the modification request is for C2 communication is FFS.

Editor's note: How the SMF determines re-authorization is required at PDU session modification is FFS.

4. The SMF informs the UAV the C2 pairing authorization result in the PDU Session Modification Command message. The SMF shall include the authorization result, optionally new CAA-level UAV ID and security information if received, to the UE in the message. The SMF then interacts with the PCF to retrieve the associated policy rules based on the authorization information provided by the USS to enable the requested C2 communication. The SMF configures the UPF based on the policy rules provided by the PCF to enable the requested C2 communication.

If C2 authorization is requested during PDU session establishment to a PDU session used specifically for connectivity to UAV-C the UAV requests C2 authorization as follows.



Figure 5.2.5.2-2: PDU Session establishment for C2 communication (separate PDU Sessions for UAS services)

1. The UAV initiates PDU Session establishment procedure for a DNN/S-NSSAI dedicated for connectivity to UAV-C. The UAV includes the pairing information as part of UAS container in the PDU Session establishment request. The USS may also use its locally configured pairing information for UAV - UAV-C pairing authorization. The pairing information includes the CAA-level UAV IDs of the requesting UAV and also includes identification information of UAV-C to pair if available. The UAS container may include other information such as Flight Authorization information.

Editor's note: How the UAV indicates that the PDU session is for C2 communication is FFS.

2. The SMF invokes the authorization procedure with the USS (via UAS-NF) as described in clause 5.2.3. The USS shall inform the SMF, through the UAS-NF as described in clause 5.2.3, the result of the authorization. If the pairing information is included in the authorization request, the authorization request is also used to request authorization to pair the UAV with UAV controller and the authorization response implicitly or explicitly indicates whether the UAV is allowed to be paired with the UAV controller. The USS determines remote identification and tracking information that may also include a new CAA-level UAV ID for the UAV during the pairing authorization procedure and send it together with the authorization result to the SMF. The SMF may receive authorization information for C2 from the USS and continues the PDU session establishment procedure. The authorization information includes UAV-C IP address.

Editor's note: How the SMF determines pairing authorization is required is FFS.

3. The SMF informs the UAV about the C2 authorization result in the PDU Session Accept or Reject message. The SMF shall include the authorization result, optionally new CAA-level UAV ID and security information if received, to the UE in the message. The SMF then interacts with the PCF to retrieve the associated policy rules based on the authorization information provided by the USS to enable the requested C2 communication. The SMF configures the UPF based on the policy rules provided by the PCF to enable the requested C2 communication.

The C2 authorization can be revoked by the USS at any time, as described in clause 5.2.9. The paired UAV-C can be replaced by a new UAV-C as described in clause 5.2.8.

\* \* \* \* Eighth change \* \* \* \*

### 5.2.7 UUAA Revocation by USS/UTM



Figure 5.2.7.1-1: Procedure for UAV authorization revocation by USS.

UAS NF stores the UAV UEs UUAA context after successful UUAA procedure as explained in clause 5.2.2.2 for UUAA-MM and in clause 5.2.3.2 for UUAA-SM procedure. The UUAA context may be stored in the UDSF or may be stored locally in the UAS NF depending on deployments. The UAS NF shall also create an implicit subscription for notification towards the AMF (in UUAA-MM) or SMF (in UUAA-SM) after the successful UUAA procedure. This notification is used by the UAS NF to trigger re-authentication, update authorization data or revoke authorization of the UAV, upon receipt of such request from the USS.

1. The USS sends an authorization revocation request to UAS NF. The USS includes GPSI, CAA-Level UAV ID, PDU Session IP address if available in the authorization revocation request.

2. UAS NF retrieves the UAV UE's stored UUAA context. From the stored UUAA context the UAS NF determines the target AMF or SMF for sending the notification.

3a or 3b. The UAS NF sends Nnef\_Auth\_Notification request to notify the target NF, i.e. either the AMF or the SMF that the UAV is not authorized anymore.

4. The UAS NF responds back to the USS indicating that authorization revocation request has been successfully initiated.

5. If UE is in CM\_Idle state, the target NF (i.e. either the AMF or the the SMF) initiates the Network Triggered Service Request procedures as described in TS 23.502 clause 4.2.3.3.

6a. If the target NF is AMF, the AMF initiates UCU procedure to inform the UE that UUA is revoked. The AMF shall also initiate the release of PDU Sessions related to C2 communication.

6b. If the target NF is AMF, based on network policy the AMF may start network initiated de-registration process as described in clause 4.2.2.3.3 in TS 23.502.

6c. If the target NF is SMF, the SMF starts network initiated PDU session release process as described in clause 4.3.4 of TS 23.502 to release the associated PDU session.

\* \* \* \* End of changes \* \* \* \*