ETSI TS 133 256 V17.1.0 (2022-07)

5G;
Security aspects of Uncrewed Aerial Systems (UAS)
(3GPP TS 33.256 version 17.1.0 Release 17)

Reference
RTS/TSGS-0333256vh10

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

1 Scope

The present document specifies the security features in support of the architecture enhancements for supporting Uncrewed Aerial Systems (UAS) connectivity, identification, tracking and pairing authorization defined in TS 23.256 [3], according to the use cases and service requirements defined in TS 22.125 [6].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".

[4] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[6] 3GPP TS 22.125: "Uncrewed Aerial System (UAS) support in 3GPP".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms 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].

3GPP UAV ID: as defined in TS 23.256 [2].

CAA (Civil Aviation Administration)-Level UAV Identity: as defined in TS 23.256 [2].

Command and Control (C2) Communication: as defined in TS 23.256 [2].

UAS NF: as defined in TS 23.256 [2].

UAS Service Supplier (USS): as defined in TS 23.256 [2].

UAS Traffic Management (UTM): as defined in TS 23.256 [2].

UAS Services: as defined in TS 23.256 [2].

Uncrewed Aerial System (UAS): as defined in TS 23.256 [2].

UUAA: as defined in TS 23.256 [2].

UUAA-MM: as defined in TS 23.256 [2].

UUAA-SM: as defined in TS 23.256 [2]..

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

UAS	Uncrewed Aerial System
UAV	Uncrewed Aerial Vehicle
USS	UAS Service Supplier
UTM	UAS Traffic Management

4 Overview

TS 23.256 [3] describes the architecture enhancements for supporting Uncrewed Aerial Systems (UAS).TS 23.256 [3] contains the reference architecture and message flows to support this new functionality for UAVs. The present document describes the security of these new features including:

- Authentication and authorization of a Uncrewed Aerial Vehicle (UAV) with the UAS Service Supplier (USS) during 5GS registration;
- Authentication and authorization of a PDU session establishment and PDN connection establishment with the USS;
- Support re-authentication, re-authorisation and revocation of the above;
- Support for USS authorization of pairing of UAVs and UAV-Cs; and
- Support for authorisation of providing location information and providing network based location to mitigate against UAVs reporting false location data.

5 Security procedures for UAS

5.1 General

Clause 5 contains the security details for the various UAS features that are given in TS 23.256 [3].

NOTE: Protection of UAS traffic is the responsibility of the USS/UAV provider and these should ensure that this data is protected independently of any protection provided by the 3GPP network as this ensures that data is protected in all cases.

5.2 UUAA

5.2.1 UUAA in 5GS

5.2.1.1 General

The UAV USS authentication and authorization (UUAA) is the procedure to ensure that the UAV can be authenticated and authorized by a USS before the connectivity for UAS services is enabled. This clause specifies the relationship

between primary authentication (as described in clause 6.1 in TS 33.501 [2]) and UUAA. An UAV is allowed to perform UUAA with the USS/UTM only after the UAV (UE) has completed successfully primary authentication.

It may be triggered by the AMF when UAV is registering with 5GS or triggered by the SMF during the PDU session establishment procedure. The UUAA procedure may also be triggered by a USS for re-authentication if the USS had authenticated the UAV. Network support for UUAA during registration is optional while it is mandatory during the PDU Session establishment. UE Support for UUAA during registration and during the PDU Session establishment is mandatory.

The AMF or SMF triggers the UUAA procedure if the UAV has an Aerial UE subscription and the UAV requests access to UAS services by providing the CAA-Level UAV ID of the UAV in the Registration Request or PDU Session Establishment Request.

The UUAA is performed between the UAV and the USS. The UAV is authenticated based on the CAA-Level UAV ID and credentials associated to the CAA-Level UAV ID. The authentication messages are included in a transparent container and conveyed between the UAV and the USS via a 3GPP UAS NF.

NOTE: The provision of CAA-Level UAV ID, credentials, and the actual authentication methods and information that needs to be sent to perform the UUAA are out of scope of the 3GPP specifications.

On successful completion of a UUAA, the USS can send UAS security information in the UUAA Authorization Payload to the UAV. The contents of that security information are out of scope of the 3GPP specifications.

The UUAA procedure at registration in 5G is described in the clause 5.2.1.2 and the UUAA procedure during PDU session establishment procedure is described in the clause 5.2.1.3.

At any time after the initial registration, the USS or the AMF (when the networking supports UUAA during registration) may initiate the Re-authentication procedure for the UAV. The AMF initiated Re-authentication procedure is described in the clause 5.2.1.2, whereas the USS initiated Re-authentication procedure is described in the clause 5.1.2.4.

Figure 5.2.1.1-1 provides an example of how UUAA fits into the 5GS procedures. The complete description of this flow is given in TS 23.256 [3].

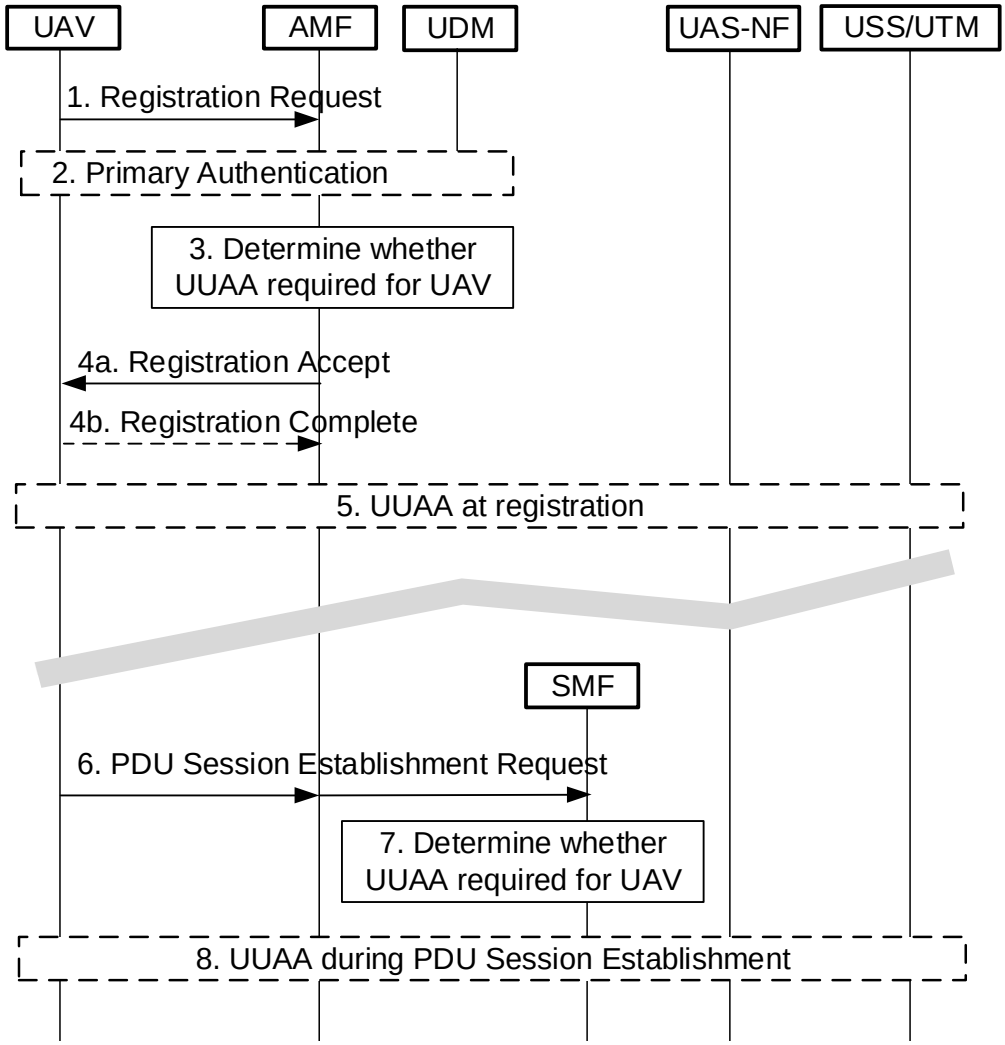

Figure 5.2.1.1-1: UUAA in 5GS

1. The UE sends a Registration Request message to the AMF. The UE may provide a CAA-Level UAV ID, and optionally a USS address/IP address, to indicate the request is registering for UAS services. In case the CAA-Level UAV ID and/or USS address/IP address is configured not to be sent in plain text, e.g., the USS address or an IP address not to be exposed in public, the CAA-Level UAV ID, and USS/IP address if available, shall be sent after the NAS security is established.

2. AMF completes security set up including primary authentication as needed.

3. After successful Primary authentication, AMF determines whether UUAA is required for the UE. UUAA shall only be triggered if the UE has provided a CAA-Level UAV ID and has a valid Aerial UE subscription. AMF may skip UUAA if the UE has completed UUAA successfully before and the UE UUAA is current, i.e., the UE's authentication and authorization has not been revoked after a previous successful UUAA.

4a. AMF shall return a Registration Accept message to the UE and indicate that UUAA is pending.

4b. UE may send a Registration Complete message to acknowledge the AMF.

5. AMF triggers the UUAA procedure if determined needed in step 3 as described in clause 5.2.1.2.

The following procedure is for UUAA during PDU session establishment:

6. The UE sends a PDU Session Establishment Request message to the SMF including a CAA-Level UAV ID to indicate the request is for UAS services. If a successful UUAA has been performed at Registration, there is no need for the USS to perform UUAA at PDU Session establishment. When a UE sends PDU Session Establishment Request message with DNN/S-NSSAI related to UAS service, if the AMF has successful UUAA result available for the UE, the AMF shall send the successful UUAA result indication along with the PDU Session Establishment Request message to the SMF.

7. The SMF determines whether UUAA is required for the UE. UUAA shall only be triggered if the UE has provided a CAA-Level UAV ID and has a valid Aerial UE subscription. SMF may skip UUAA, if it receives successful UUAA result from the AMF or the UE has completed UUAA successfully with the same USS/DN before, i.e., at registration as in step 5 or in previous PDU Session Establishment procedures.

8. The SMF triggers the UUAA procedure if determined needed at step 7 as described in clause 5.2.1.3.

5.2.1.2 UUAA Procedure at Registration

The UUAA procedure at registration is triggered by an AMF with the details described below, which considers only the security related parameters (see TS 23.256 [3] for full details of the flows). For an AMF initiated re-authentication, the procedure starts from the step 2.

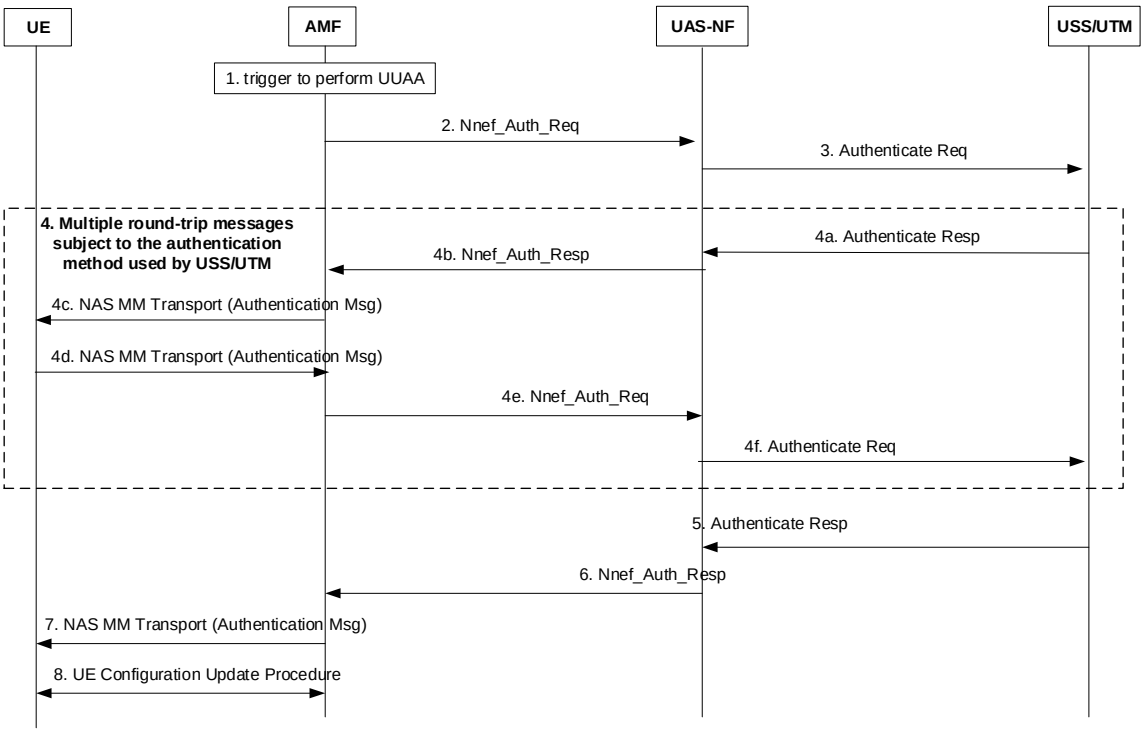

Figure 5.2.1.2-1: UUAA Procedure at Registration

1. The AMF triggers the UUAA procedure as described in clause 5.2.1.1.

2. The AMF sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the Aviation Payload if provided by the UE for USS to authenticate the UAV. The AMF may include other information in the request as in TS 23.256 [3].

3. The UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address. Only authorized USS shall be used in order to ensure only legitimate entities can provide authorization for UAVs. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID, a UAS NF Routing information (e.g., an FQDN or IP address) which uniquely identifies the UAS NF located in the 3GPP network that handles the UAV related messages exchanges with the corresponding external USS/UTM and the transparent container. Other information may also be included in this message as in TS 23.256 [3].

4. The USS and the UE exchange Authentication messages:

NOTE 1: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by the USS. The method used to authenticate the UE (e.g. whether over EAP or not) and the content of Authentication Messages (e.g. EAP packets) to support that method are out of scope of 3GPP. The USS determines the authentication method used.

4a. The USS replies to UAS NF with the Authentication Response message. It shall include the GPSI and a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container received in 4a to the AMF with the GPSI.

4c. The AMF forwards the transparent container to the UE over NAS MM transport messages.

4d. The UE responds to the AMF with an Authentication message embedded in a transparent container over a NAS MM transport message.

4e. The AMF sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container provided by the UE.

4f. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID and the transparent container.

5. The USS sends the UAS NF an Authentication Response message. The Authentication Response shall include the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and a UUAA Authorization Payload that contains UAS security information if the USS has such information to send.

NOTE 2: The content of security information (e.g. key material to help establish security between UAV and USS/UTM) is not in 3GPP scope.

The UAS NF stores the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

NOTE 3: The USS Identifier is used to ensure that a USS requesting a subsequent re-authentication or revocation is the same one that authenticated the UAV in the first place. The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

6. The UAS NF sends the AMF an Authentication Response message, including the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and the UUAA Authorization Payload received in step 5.

7. The AMF sends to the UE the UUAA result (success/failure) received in step 6. The message(s) used in step 7 are given in TS 23.256 [3].

The AMF stores the results, together with the GPSI and the CAA-level UAV ID.

8. If UUAA result is success, the AMF sends to the UE the UUAA Authorization Payload, received in step 6, during a UCU procedure as described in TS 23.256 [3]. The UE shall store the authorization information if received such as UAS Security information along with the CAA-level UAV ID.

Editor's Note: It is FFS whether the inclusion of CAA level ID in step 6 and its storage at step 7 align with TS 23.256. As they were added for alignment purposes only, no action on this functionality is needed in stage 3 until this EN is resolved.

5.2.1.3 UUAA Procedure during PDU Session Establishment

The SMF may trigger a UUAA procedure during the PDU session establishment procedure with details described below, which considers only the security related (see TS 23.256 [3] for full details of the flows).

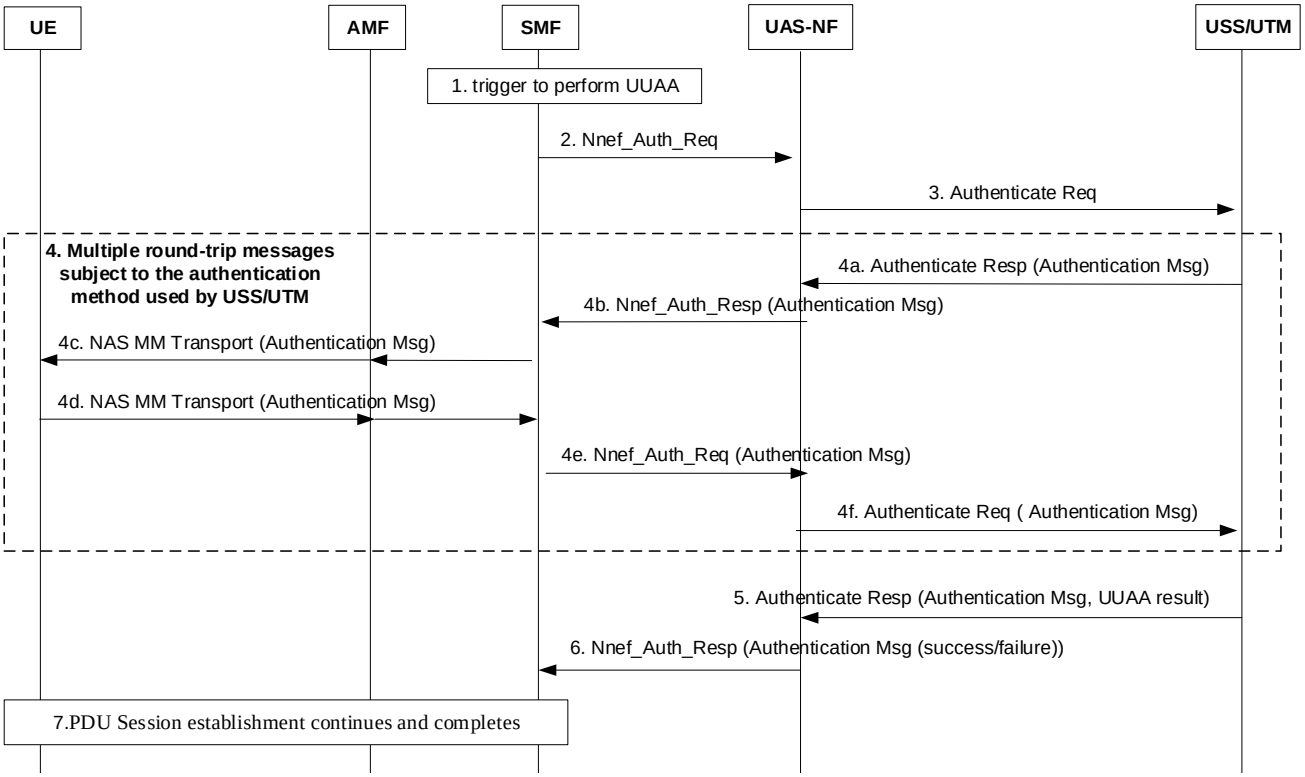

Figure 5.2.1.3-1: UUAA Procedure at PDU Session Establishment

1. The SMF determines whether UUAA is required as described in the clause 5.2.1.1 and if the UUAA result is not received from the AMF, if the UE provides a CAA-Level UAV ID indicating UAS services and optionally the Aviation Payload if provided by the UE for USS to authenticate the UAV in the PDU Session Establishment request. The SMF triggers a UUAA procedure after the determination in step 7 in the clause 5.2.1.1.

2. The SMF sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container if provided by the UE. The SMF may include other information in the request as in TS 23.256 [3].

3. The UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address. Only authorized USS shall be used in order to ensure only legitimate entities can provide authorization for UAVs. The UAS NF sends an Authentication Request to the USS which includes the GPSI, the CAA-Level UAV ID, the UAS NF Routing information (e.g., a FQDN or IP address) which uniquely identifies the NF located in the 3GPP network that handles the UAV related messages exchanges with the corresponding external USS/UTM, and the transparent container. Other information may also be included in this message (see TS 23.256 [3]).

4. The USS and the UE exchange multiple Authentication messages:

NOTE 1: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by the USS. The method used to authenticate the UE (e.g. whether over EAP or not) and the content of Authentication Messages (e.g. EAP packets) to support that method are out of scope of 3GPP. The USS determines the authentication method used.

4a. The USS replies to UAS NF with the Authentication Response message. It shall include the GPSI, a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container to the SMF.

4c. The SMF forwards the transparent container to the AMF, which then forwards to the UE over a NAS MM transport message.

4d. The UE responses the AMF with an Authentication message embedded in a transparent container over a NAS MM transport message. The AMF forwards to the SMF.

4e. The SMF sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container provided by the UE.

4f. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID and the transparent container.

NOTE 2: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by USS. The method used to authenticate the UE and the content of Authentication Messages are out of scope of 3GPP.

5. The USS sends the UAS NF an Authentication Response message. The Authentication Response shall include the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and a UUAA Authorization Payload that contains UAS security information if the USS has such information to send to the UAV.

NOTE 3: The content of security information (e.g., key material to help establish security between UAV and USS/UTM) is not in 3GPP scope.

If UUAA successful, the UAS NF stores the UAV UEs' UUAA context, including the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

NOTE 4: The USS Identifier is used to ensure that a USS requesting a subsequent re-authentication or revocation is the same one that authenticated the UAV in the first place. The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

6. The UAS NF sends the SMF an Authentication Response message, including the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and the UUAA Authorization Payload received in step 5.

The SMF stores the results, together with the GPSI and the CAA-level UAV ID.

7. The SMF sends the UUAA result (success/failure), and the UUAA Authorization Payload received in step 5 to the UE. The message(s) used in step 7 and any further actions the UE and SMF take are given in TS 23.256 [3].

8. The UE on receiving the UUAA result as success, shall store the authorization information if received such as, CAA-level UAV ID, and UAS Security information.

Editor's Note: It is FFS whether the inclusion of CAA level ID in step 6 and its storage at step 7 align with TS 23.256. As they were added for alignment purposes only, no action on this functionality is needed in stage 3 until this EN is resolved.

5.2.1.4 UUAA re-authentication procedure (5G)

As described in clause 5.2.1.1, the USS or the AMF (if support UUAA during registration) may initiate the Re-authentication procedure for the UAV at any time.

This clause describes the USS initiated Re-authentication procedure (the AMF initiated Re-authentication procedure is described in the clause 5.2.1.2). The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).

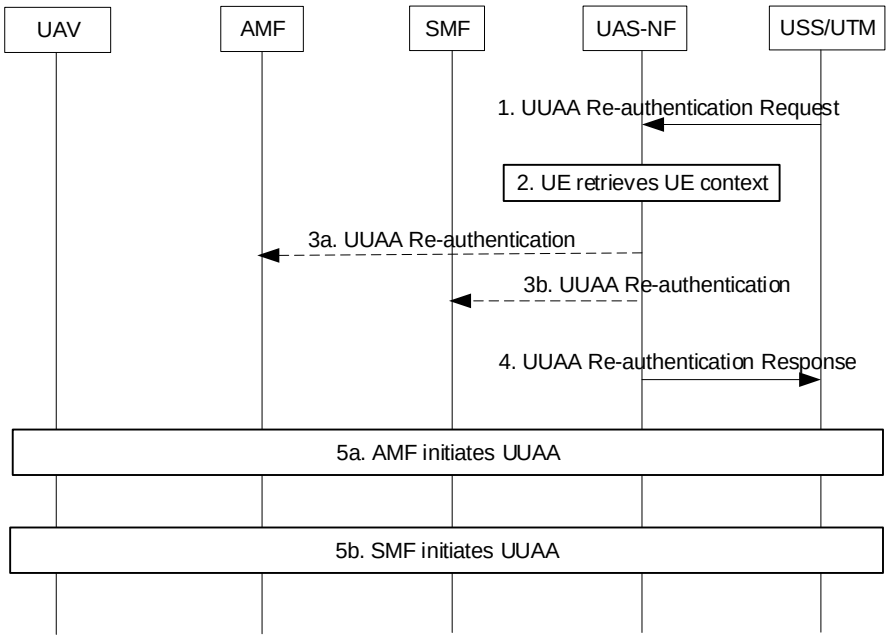

Figure 5.2.1.4-1: UUAA re-authentication in 5GS

1. The USS sends a re-authentication request for the UAV to UAS-NF that includes GPSI, CAA-Level UAV ID, and an authentication message. It may contain the PDU Session IP address if available. The USS shall use the UAS NF Routing information received during the previous successful UUAA related to GPSI for sending the re-authentication request.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UAA. The UAS-NF verifies the USS re-authentication request by checking whether the GPSI and the USS identifier match of the USS requesting the re-authentication the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the re-authentication procedures if match.

NOTE 1: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

The UAS NF determines whether the target NF is an AMF or an SMF.

- If the target NF is an AMF, the UAS NF further determines the target AMF for re-authentication and continues step 3a.

- If the target NF is an SMF, the UAS NF further determines the target SMF for re-authentication and continues step 3b.

3a or 3b. The UAS NF sends to either the target AMF or the target SMF the UAA re-authentication request for the UE identified by the GPSI and for the SMF only the PDU Session IP address if available.

4. The UAS NF responses the USS that the UAA Re-authentication has been initiated.

5a. If the target NF is an AMF, the AMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.2 (step 2 to step 9).

5b. If the target NF is an SMF, the SMF initiates re-authentication of the UAV as UUAA described in the clause 5.2.1.3 (step 2 to step 7).

5.2.1.5 UUAA Revocation

USS may trigger revocation of UUAA at any time. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).

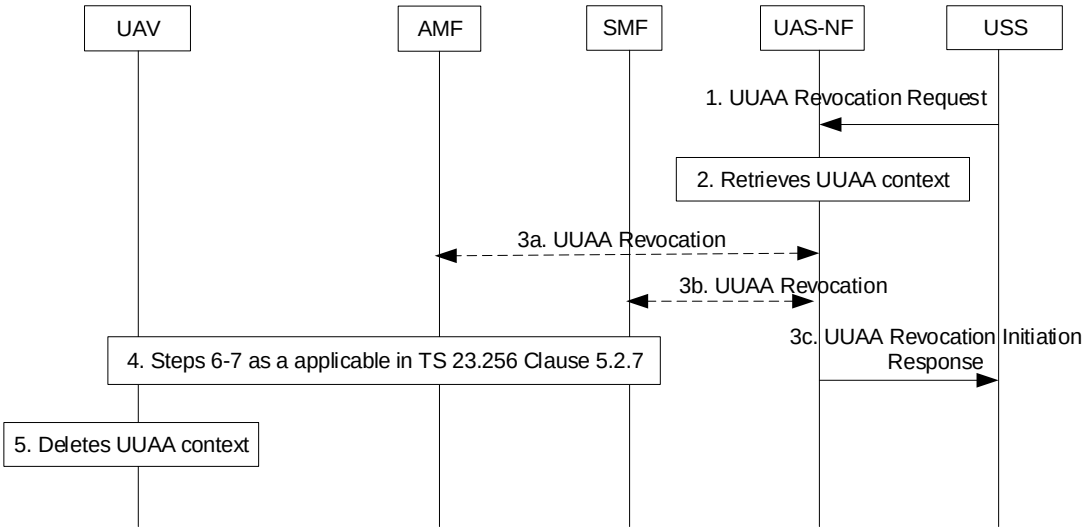

Figure 5.2.1.5-1: UUAA revocation in 5GS

1. The USS sends an UUAA revocation request to UAS-NF. The request includes GPSI and CAA-Level UAV ID.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UUAA. The UAS-NF verifies the USS revocation request by checking whether the GPSI and the USS identifier of the USS requesting the revocation match the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the revocation procedures if they match.

NOTE 1: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. , the identity mapped during link establishment or the identity in certificate).

The UAS NF determines whether the target NF is an AMF or an SMF.

- If the target NF is an AMF, the UAS NF further determines the target AMF for revocation and continues step 3a.
- If the target NF is an SMF, the UAS NF further determines the target SMF for revocation and continues step 3b.

3a or 3b. The UAS NF sends to either the target NF, i.e., the target AMF or the target SMF the UUAA revocation message for the UE identified by the GPSI and the PDU session identified by the GPSI and the IP address. The target NF (i.e., the target AMF or the target SMF) shall respond to the UAS NF to indicate the revocation has been successful.with the GPSI and success indication.

3c. The UAS NF responds back to the USS indicating that authorization revocation request has been successfully initiated as in TS 23.256 and the UAS NF shall delete the UUAA context.

4. The target NF i.e., either the target AMF or the target SMF on receiving UUAA revocation notification message, determines to send UUAA revocation indication to the UE. The target NF (either an AMF or an SMF) informs the UE that UUAA is revoked and takes actions as described in TS 23.256 [3] with the following adaptations.

4a. If the target NF is AMF, the AMF shall send UUAA revocation indication in the UCU procedure as described in TS 23.526 Clause 5.2.7 and the AMF shall delete the UUAA context being revoked.

4b. If the target NF is SMF, the SMF shall send UUAA revocation indication in a network initiated PDU session release process as described in TS 23.526, clause 5.2.7 and the SMF shall delete the UUAA context being revoked.

5. The UE on receiving UAA revocation indication shall delete all UUAA related authorization data corresponding to the CAA-Level-UAV ID and the UE sends an UUAA revocation acknowledgement to the target NF which provided the UUAA revocation indication.

Editor's Note: It is FFS, if the 3GPP network need to provide the CAA-level UAV ID to the UAV when provided by the USS for the revocation.

5.2.2 UUAA in EPS

5.2.2.1 General

The UAV USS authentication and authorization (UUAA) is the procedure to ensure that the UAV can be authenticated and authorized by a USS before the connectivity for UAS services is enabled. This clause specifies the relationship between authentication and UUAA. An UAV is allowed to perform UUAA with the USS/UTM only after the UAV (UE) has completed successfully authentication with EPC. The SMF+PGW-C triggers the UUAA procedure if the UAV has an Aerial UE subscription and the UAV requests access to UAS services by providing the CAA-Level UAV ID of the UAV when attaching to the network.

The UUAA is performed between the UAV and the USS. The UAV is authenticated based on the CAA-Level UAV ID and credentials associated to the CAA-Level UAV ID. The authentication messages are included in a transparent container and conveyed between the UAV and the USS via a 3GPP UAS NF.

NOTE: The provision of CAA-Level UAV ID, credentials, and the actual authentication methods and information that needs to be sent to perform the UUAA are out of scope of the 3GPP specifications.

On successful completion of a UUAA, the USS sends UAS security information (if determined by the USS) in the UUAA Authorization Payload to the UAV. The contents of that security information are out of scope of the 3GPP specifications.

The UUAA procedure is described in the clause 5.2.2.2.

5.2.2.2 UUAA procedure

The UUAA procedure is triggered by an SMF+PGW-C with the details described below, which considers only the security related parameters (see TS 23.256 [3] for full details of the flows).

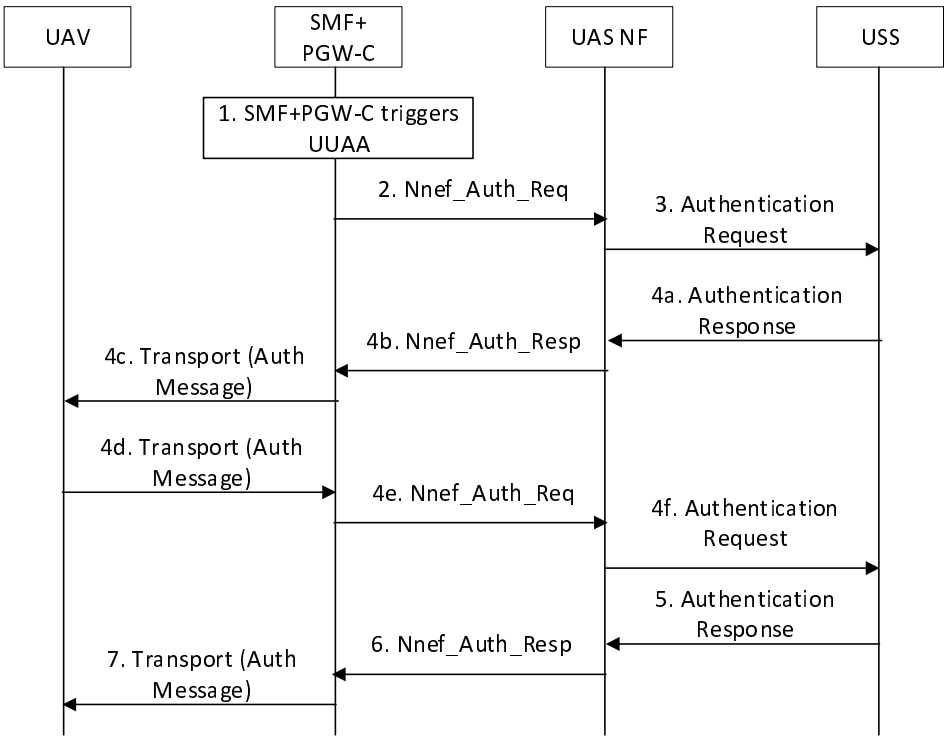

Figure 5.2.2.2-1: UUAA procedure

1. The SMF+PGW-C decides to trigger the UUAA procedure as described in TS 33.256 [3].

2. The SMF+PGW-C sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the Aviation Payload if provided by the UE for USS to authenticate the UAV. The SMF+PGW-C may include other information in the request as in TS 23.256 [3].

3. The UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address. Only authorized USS shall be used in order to ensure only legitimate entities can provide authorization for UAVs. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID, a UAS NF Routing information (e.g., a FQDN or IP address) which uniquely identifies the UAS NF located in the 3GPP network that handles the UAV related messages exchanges with the corresponding external USS/UTM and the transparent container. Other information may also be included in this message as in TS 23.256 [3].

4. The USS and the UE exchange Authentication messages:

NOTE 1: Multiple round-trip messages (4a to 4f) may be needed as required by the authentication method used by the USS. The method used to authenticate the UE (e.g. whether over EAP or not) and the content of Authentication Messages (e.g. EAP packets) to support that method are out of scope of 3GPP. The USS determines the authentication method used.

4a. The USS replies to UAS NF with the Authentication Response message. It shall include the GPSI and a transparent container composed of an authentication message.

4b. The UAS NF sends the transparent container received in 4a to the SMF+PGW-C with the GPSI.

4c. The SMF+PGW-C forwards the transparent container to the UE over NAS MM transport messages.

4d. The UE response to the SMF+PGW-C with an Authentication message embedded in a transparent container over a NAS MM transport message.

NOTE 2: The method of transporting messages between the SMF+PGW-C and UE is described in TS 23.256 [3].

4e. The SMF+PGW-C sends a message Nnef_Auth_Req to the UAS NF, including the GPSI and the CAA-Level UAV ID, and the transparent container provided by the UE.

4f. The UAS NF sends an Authentication Request to the USS. The Authentication Request shall include the GPSI, the CAA-Level UAV ID and the transparent container.

5. The USS sends the UAS NF an Authentication Response message. The Authentication Response shall include the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and a UUAA Authorization Payload that contains UAS security information if the USS has such information to send.

NOTE 3: The content of security information (e.g. key material to help establish security between UAV and USS/UTM) is not in 3GPP scope.

NOTE 4: The USS Identifier is used to ensure that a USS requesting a subsequent re-authentication or revocation is the same one that authenticated the UAV in the first place. The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

The UAS NF stores the GPSI, USS Identifier (and the binding with the GPSI) and the CAA-level UAV ID (and the binding with the GPSI).

6. The UAS NF sends the SMF+PGW-C an Authentication Response message, including the GPSI, the UUAA result (success/failure), the authorized CAA-level UAV ID, and the UUAA Authorization Payload received in step 5.

7. The SMF+PGW-C sends to the UE the UUAA result (success/failure) and the UUAA Authorization Payload received in step 5. The message(s) used in step 7 and any further actions the SMF+PGW-C takes are given in TS 23.256 [3].

The SMF+PGW-C stores the results, together with the GPSI and the CAA-level UAV ID.

8. If UUAA result is success, the UE shall store the authorization information if received such as UAS Security information along with the CAA-level UAV ID.

Editor's Note: It is FFS whether the inclusion of CAA level ID in step 6 and its storage at step 7 align with TS 23.256. As they were added for alignment purposes only, no action on this functionality is needed in stage 3 until this EN is resolved.

5.2.2.3 UUAA re-authentication procedure (EPC)

The USS the Re-authentication procedure for the UAV at any time. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).

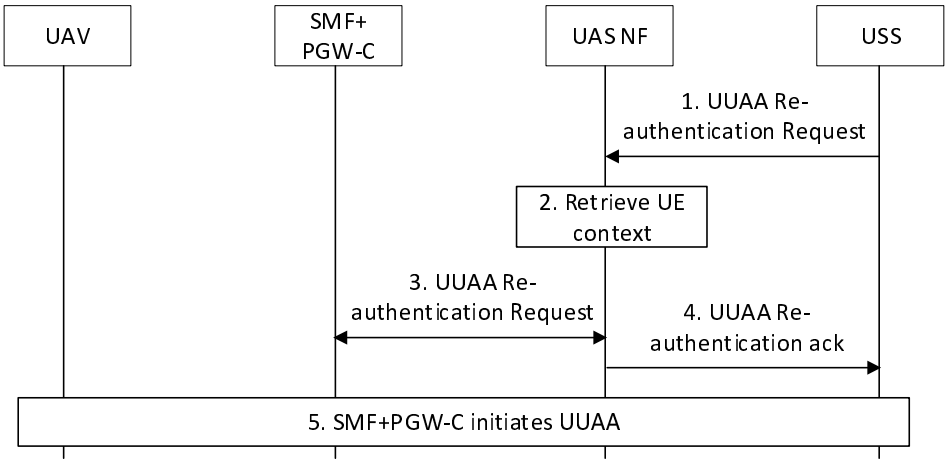

Figure 5.2.2.3-1: UUAA re-authentication in EPS

1. The USS sends a re-authentication request for the UAV to UAS-NF that includes GPSI, CAA-Level UAV ID, and an Authentication message. It may contain the PDU Session IP address if available. The USS shall use the UAS NF Routing information received during the previous successful UUAA related to GPSI for sending the re-authentication request.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UAA. The UAS-NF verifies the USS re-authentication request by checking whether the GPSI and the USS identifier of the USS requesting the re-authentication match the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the re-authentication procedures if match.

NOTE 1: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

3. The UAS NF sends to the target SMF+PGW-C the UAA re-authentication request for the UE identified by the GPSI.

4. The UAS NF responses the USS that the UAA Re-authentication has been initiated.

5. The SMF+PGW-C initiates re-authentication of the UAV as UUAA described in the clause 5.2.2.2 (step 4c to step 7).

5.2.2.4 UUAA Revocation

USS may trigger revocation of UUAA at any time. The below description considers only the security related parameters (for full details of the flows see TS 23.256 [3]).

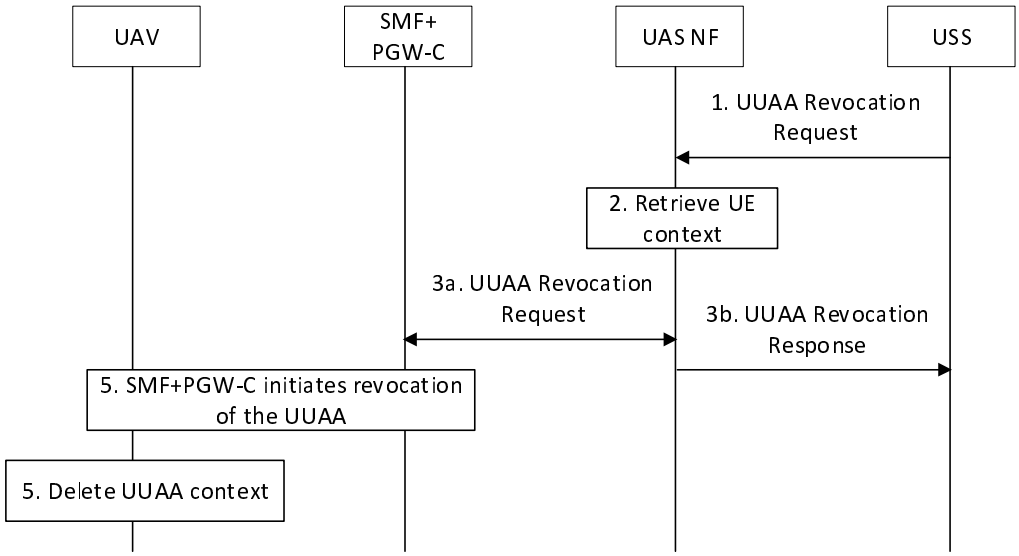

Figure 5.2.2.4-1: UUAA revocation in EPS

1. The USS sends an UUAA revocation request to UAS-NF. The request includes GPSI and CAA-Level UAV ID.

2. The UAS NF retrieves the UAV UE's context. The UE's context contains identity mapping between the GPSI and the USS identifier that performed UUAA. The UAS-NF verifies the USS revocation request by checking whether the GPSI and the USS identifier of the USS requesting the revocation match the stored mapping of GPSI and USS identifier. The UAS-NF shall only continue the revocation procedures if they match.

NOTE: The USS identifier is based on the security link on the interface between USS NF and USS (e.g. the identity mapped during link establishment or the identity in certificate).

3a. The UAS NF sends to the target SMF+PGW-C, the UUAA revocation message for the UE identified by the GPSI. The target SMF+PGW-C shall respond to the UAS NF to indicate the revocation has been successful.

3b. The UAS NF responds back to the USS indicating that authorization revocation request has been successfully initiated as in TS 23.256 [3] and the UAS NF shall delete the UUAA context.

4. The target SMF+PGW-C on receiving UUAA revocation notification message, determines to send UUAA revocation indication to the UE. The target SMF+PGW-C informs the UE that UUAA is revoked and takes actions as described in TS 23.256 [3] and the SMF+PGW-C shall delete the UUAA context being revoked.

5. The UE on receiving UAA revocation indication shall delete all UUAA related authorization data corresponding to the CAA-Level-UAV ID.

Editor's Note: It is FFS, if the 3GPP network need to provide the CAA-level UAV ID to the UAV when provided by the USS for the revocation.

5.3 Location Information Veracity and Location Tracking Authorization

5.3.1 General

There are three UAV tracking modes as follows (see TS 23.256 [3] for more details):

- UAV location reporting mode;
- UAV presence monitoring mode; and
- Unknown UAV tracking mode.

The first two relate to obtaining location information about a particular UE while the latter one is about obtaining information about all the UEs in a particular geographic region.

For the first two mode before proceeding with the request for information about the particular UE, the UAS NF shall ensure that the requesting USS is the one that authorized the UE.

For the latter mode, a USS is authorized to receive the CAA level ID of all UAVs in a geographic area indicated by the USS. In addition, if the USS performed the UUAA of the UAV, or the UAS NF is configured to know the USS is authorized to receive such information, then the 3GPP UAV ID of such UAVs is also included.

5.3.2 Location information veracity and location tracking authorization in 5GS

USS may receive the location information which is reported by UAV via the application layer. The USS may decide to check and verify the location information in order to prevent spoofed and forged location information. The location result from 5GS helps to verify the location information reported from UAV side. 5GS provides network-based location information by utilizing the Location Services (LCS) supported by AMF or GMLC as specified in TS 23.273 [4] and 23.502 [5], and the detailed procedures of location information veracity and location tracking authorization are described below.

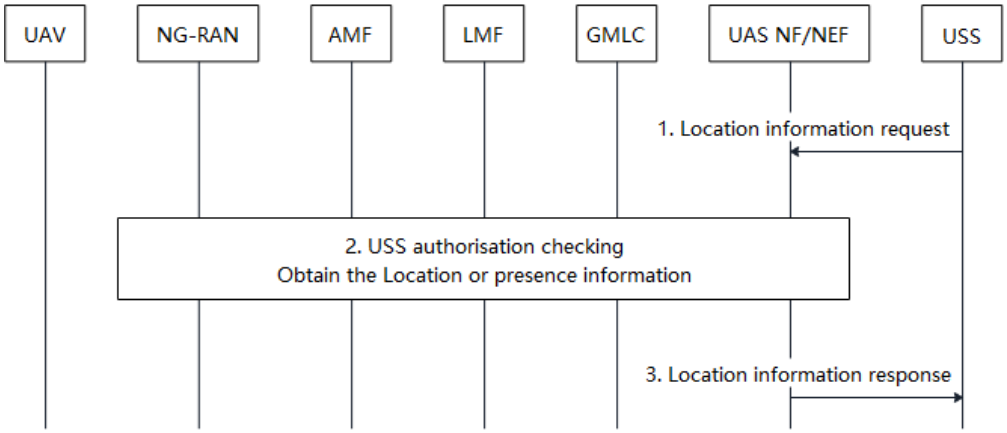

Figure 5.3.2-1: Location information veracity and location tracking authorization in 5GS

Step 1-3 shows the procedure for the USS to obtain a network-based location for UAV(s).

1. The USS sends the location request to UAS NF/NEF to request the UAV location or presence from network. The location request includes the GPSI of the UAV to request the location information or presence about an individual UE, or a geographic area when trying to find the information of all UAVs in an area. The LCS request also indicates the 5GS to obtain reliable UE location information, i.e. the location calculated and provided by the network.

   If the USS/TPAE does not specify target 3GPP UAV ID and request UAS NF for a list of the UAVs in the geographic area and served by the PLMN, clauses 5.3.1.3 and 5.3.4 in TS 23.256 [3] apply.

2. The UAS NF/NEF first verifies the request in step 1 is authorized. When the USS sends a GPSI, this is done by checking whether the identifier of the USS sending the request matches the previously associated mapping between the GPSI and the USS identifier. When the USS request UAS NF for a list of the UAVs in the geographic area, this is done by checking the USS is authorized to receive the CAA level ID of all UAVs in a geographic area indicated by the USS. The UAS NF/NEF gets the relevant UAV(s) location information or presence from AMF or GMLC by the current location services supported by AMF or GMLC if passes the above authorization check. On the condition of the location services provided by AMF, the UE presence status is provided by reusing the Area of Interest mechanism. On the condition of the location services provided by GMLC, the GMLC indicates LMF via AMF to select Network Assisted Positioning method which relies on the location measurement from NG-RAN nodes, if receiving reliable location information request in step 1.

NOTE 1: The USS may be authorized by UAS NF/NEF by means not specified in this release of the present document.

3. The UAS NF/NEF provides the UAV(s) location information or presence to the USS. When the USS request UAS NF for a list of the UAVs in the geographic area, if the USS performed the UUAA of the UAV, or the UAS

NF is authorized to receive such information, then the 3GPP UAV ID of such UAVs is also included. USS may make decisions to control the UAV based on the result output received from UAS NF/NEF.

NOTE 2: Use of LCS privacy feature (e.g. user consent) is applicable to UAVs as for normal UEs.

5.4 Pairing Authorization for UAV and UAVC

5.4.1 General

Pairing authorization in 5GS is performed during either a PDU Session Establishment procedure or a PDU Session Modification procedure.

5.4.2 UAV pairing Authorization with UAVC in 5GS

Pairing authorization may be performed during a PDU Session Establishment/PDU Session Modification after a successful UAA between the UAV and the USS/UTM. If no successful UUAA has been performed, then the pairing authorization can occur during the UUAA-SM procedure (see clause 5.2.5.2.1 of TS 23.256 [3] for full details). This procedure follows the clause 5.2.1.3 with the following additions:

- the UE provides pairing information (if available) in a C2 authorization payload in the PDU Session Establishment message and this is forwarded to the USS in steps 2 and 3; and

- after a successful authentication and before sending the message in step 5, the USS performs C2 authorization considering the included pairing information, the CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result) if the USS has such information to send. This is passed to the UE in steps 5-7. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope.

UAV pairing authorization during the PDU Session Establishment/PDU Session Modification procedure is described as follows. Full details of the procedures are given in TS 23.256 [3].

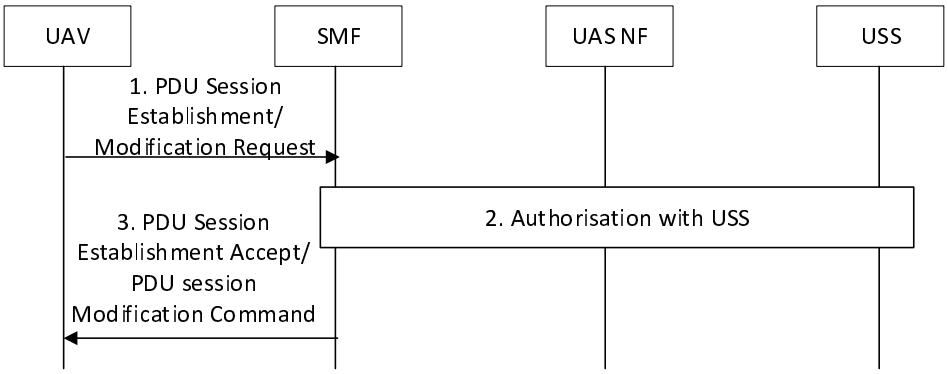

Figure 5.4.2-1: UAV pairing authorization during PDU Session Establishment

1. When the UAV needs a new dedicated PDU session for connectivity to the UAV-C, the UE initiates a PDU Session Establishment procedure. When the UE wants to use an existing PDU session for connectivity to the UAV-C, the UE initiates a PDU Session Modification procedure. The UE shall include the following IEs in the PDU session establishment/modification request: a CAA-Level UAV ID, a DNN/S-NSSAI implying dedicated connectivity to UAV-C, and UAV pairing information, which includes any needed authorization information, if available.

   The pairing information includes the CAA-level UAV IDs of the requesting UAV and identification information of UAV-C to pair. The USS may also use its locally configured pairing information for UAV and UAV-C pairing authorization which takes precedence over UAV provided pairing information.

NOTE: The integrity protection of pairing information is recommended. It is performed by the USS, and is not in scope of 3GPP system.

2. The SMF determines whether the UAV pairing authorization is required based on UAV's aerial subscription, presence of CAA-Level UAV ID, and DNN/S-NSSAI indicating the UAV service, as step 7 in clause 5.2.1.1:

   The SMF invokes the authorization procedure with the USS via UAS-NF. The USS will perform C2 authorization taking account of the included pairing information, which includes any needed authorization information, if available, the CAA-Level UAV ID, and GPSI, etc.

   The USS informs the SMF via the UAS NF of the authorization results. The authorization information includes the IP address of the UAV-C and a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result) if the USS has such information to send. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope. The other information contained in this message is given in TS 23.256 [3].

3. The SMF informs the UE the paring authorization result in the PDU Session Establishment Accept message/PDU session Modification Command, which may include a new CAA-level UAV ID. The UE shall store the Pairing authorization result and authorization information.

   The PDU Session Establishment/Modification continues and completes as described in TS 23.256 [3].

   The UAV pairing authorization can be revoked by the USS at any time.

   Besides, the paired UAV-C can be replaced by a new UAV-C by the USS at any time.

5.4.3 UAV pairing Authorization with UAVC in EPS

Pairing authorization may be performed during a PDN Connection Establishment/PDN Connection Modification procedure after a successful UUAA between the UAV and the USS/UTM. If no successful UUAA has been performed, then the pairing authorization can occur during the during the UUAA procedure (see clause 5.2.5.3.0 of TS 23.256 [3] for full details). This procedure follows the clause 5.2.2.2 with the following additions:

- the UE provides pairing information (if available) in a C2 authorization payload and this is forwarded to the USS in steps 2 and 3; and

- after a successful authentication and before sending the message in step 5, the USS performs C2 authorization considering the included pairing information, the CAA-Level UAV ID and 3GPP UAV ID/GPSI. The USS includes a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result, i.e., whether the UAV is allowed to be paired with the UAV-C) if the USS has such information to send. This is passed to the UE in steps 5-7. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope.

UAV pairing authorization during the PDN Connection Establishment/ Modification procedure is described as follows. Full details of the procedures are given in TS 23.256 [3].

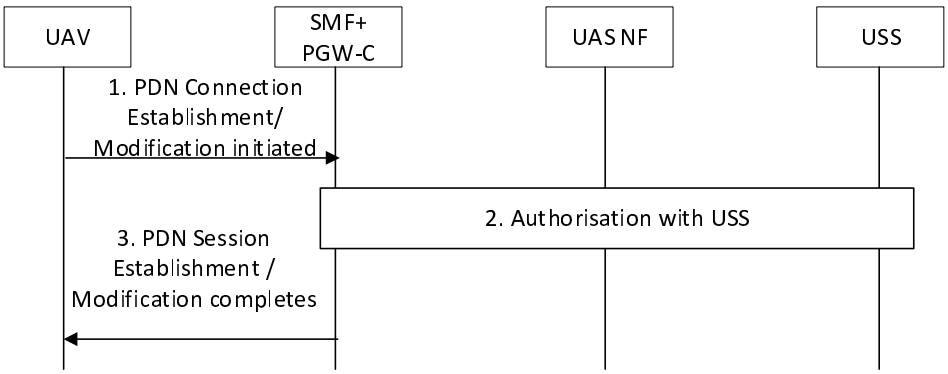

Figure 5.4.3-1: UAV pairing authorization during PDN Connection Establishment/Modification

1. When the UAV needs a new dedicated PDU session for connectivity to the UAV-C, the UE initiates a PDN Connection Session Establishment procedure. When the UAV needs to use an existing PDN connection for connectivity to the UAV-C, the UE initiates a PDN Connection Modification procedure. The UE shall include

the following IEs in the PDN connection establishment/modification request: a CAA-Level UAV ID, a DNN/S-NSSAI implying dedicated connectivity to UAV-C, and UAV pairing information, which includes any needed authorization information, if available.

The pairing information includes the CAA-level UAV IDs of the requesting UAV and identification information of UAV-C to pair. The USS may also use its locally configured pairing information for UAV and UAV-C pairing authorization which takes precedence over UAV provided pairing information.

NOTE: The integrity protection of pairing information is recommended. It is performed by the USS, and is not in scope of 3GPP system.

2. The SMF+PGW-C determines whether the UAV pairing authorization is required based on UAV's aerial subscription, presence of CAA-Level UAV ID, and DNN/S-NSSAI indicating the UAV service:

   The SMF+PGW-C invokes the authorization procedure with the USS via UAS-NF. The USS will perform C2 authorization taking account of the included pairing information, which includes any needed authorization information, if available, the CAA-Level UAV ID, and GPSI etc.

   The USS informs the SMF+PGW-C via the UAS NF of the authorization results. The authorization information includes the IP address of the UAV-C and a C2 authorization payload that contains C2 session security information and possibly other non-security specific information (e.g. C2 authorization result, i.e., whether the UAV is allowed to be paired with the UAV-C) if the USS has such information to send. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope. The other information contained in this message is given in TS 23.256 [3].3. The SMF+PGW-C sends the UE the C2 authorization payload with the paring authorization result and may also send a new CAA-level UAV ID. The UE shall store the Pairing authorization result and authorization information.

   The PDN Connection Establishment/Modification continues and completes as described in TS 23.256 [3].

   The UAV pairing authorization can be revoked by the USS at any time.

   Besides, the paired UAV-C can be replaced by a new UAV-C by the USS at any time.

5.5 Security for UAS NF to USS interface

The security requirements for the UAS-NF shall follow clause 5.9.2.3 in TS33.501 [2].

The UAS NF to USS interface shall be protected as described in clause 12 of TS 33.501 [2].

NOTE: Based on the architectural reference model described in TS 23.256 [3], the UAS-NF is treated as an NEF whereas the USS is treated as an external AF.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2022-03	SA#95e					Upgrade to change control version and EditHelp review	17.0.0
2022-06	SA#96	SP-220552	0004	1	F	Correction to Clause 5.2.1.5 UUAA Revocation	17.1.0
2022-06	SA#96	SP-220552	0005	1	F	Correction to Clause 5.2.2.4 UUAA Revocation	17.1.0
2022-06	SA#96	SP-220552	0006	1	F	Resolving of EN in Clause 5.2.1.4 UUAA re-authentication procedure	17.1.0
2022-06	SA#96	SP-220552	0007	-	F	Adding terms and abbreviations	17.1.0
2022-06	SA#96	SP-220552	0008	1	F	Adding text for the Overview clause	17.1.0
2022-06	SA#96	SP-220552	0012	-	F	Removing EN on USS authorisation	17.1.0
2022-06	SA#96	SP-220552	0013	-	F	Removing EN on TPAE	17.1.0
2022-06	SA#96	SP-220552	0014	1	F	Clarification on 'high reliability' location information	17.1.0
2022-06	SA#96	SP-220552	0015	1	F	Resolving the ENs on protection of UAS data	17.1.0

History

Document history		
V17.0.0	May 2022	Publication
V17.1.0	July 2022	Publication