ETSI TS 133 256 V17.2.0 (2023-01)

5G;
Security aspects of Uncrewed Aerial Systems (UAS)
(3GPP TS 33.256 version 17.2.0 Release 17)

Reference
RTS/TSGS-0333256vh20

Keywords
5G

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].

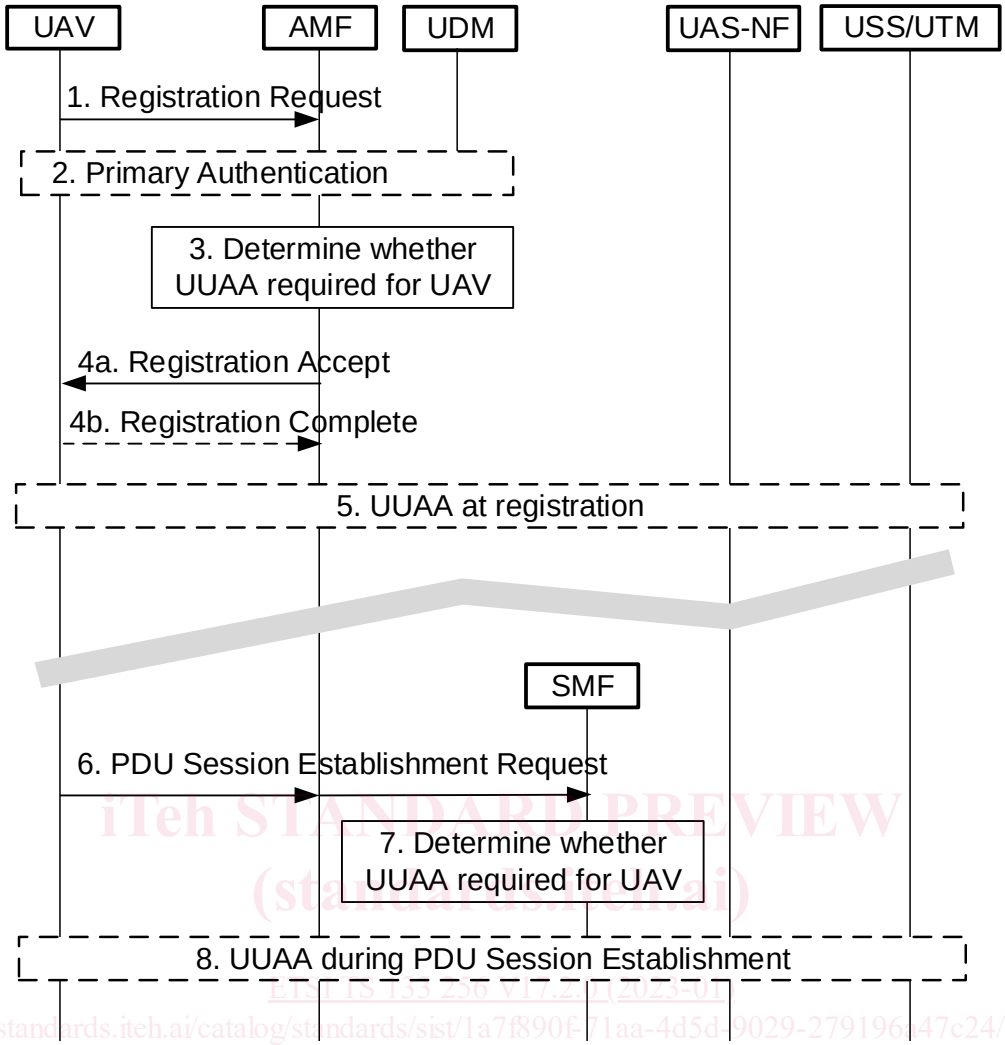

Figure 5.2.1.1-1: UUAA in 5GS

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.

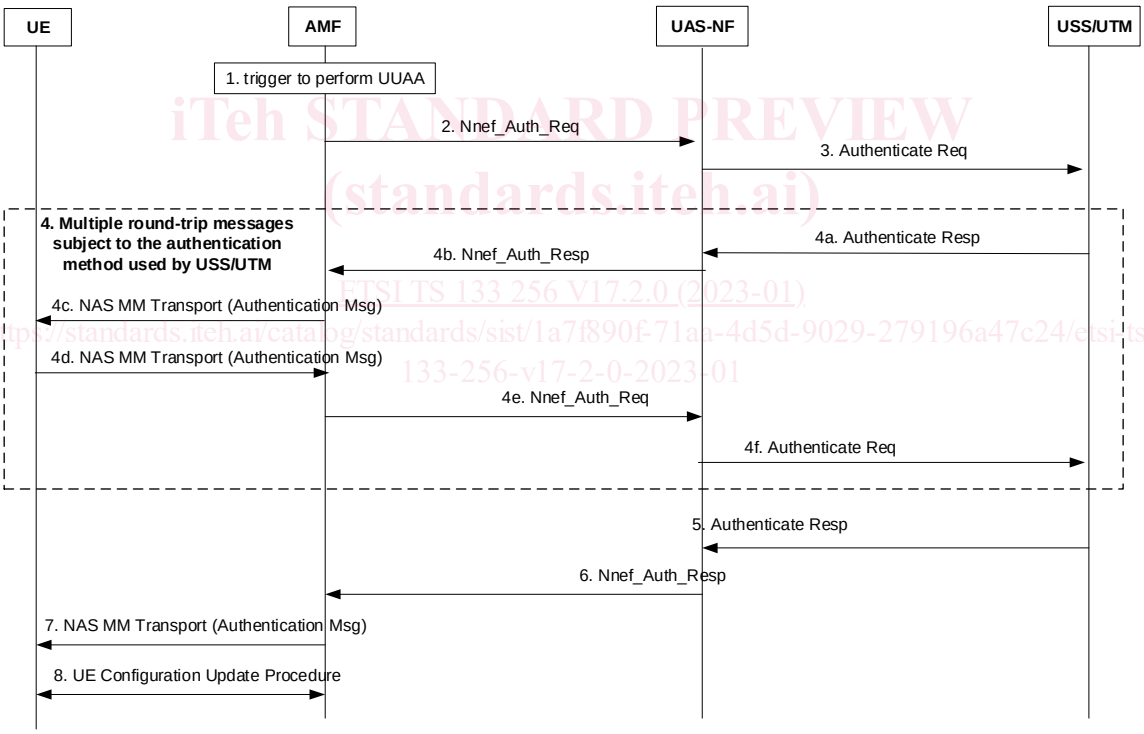

Figure 5.2.1.2-1: UUAA Procedure at Registration

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].