3GPP TR 33.854 V0.6.0 (2021-05)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects of Unmanned Aerial Systems (UAS) (Release 17)

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report 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 contains a study on the security aspects of Unmanned Aerial Systems (UAS). TS 22.125 [2] contains the service requirements for UAS while TR 23.754 [3] is studying aspects like the UAS connectivity, identification and tracking and TR 23.755 [4] studies UAV services and application layer features. The security study of the present document provides key issue including security threat and potential requirements related to the work in these other specifications and develops and analyses solutions to these key issues. Finally the study provides some conclusions for potential normative work.

Editor's note: It is FFS which of the communications in a UAS system are in the scope of SA3 and require a standardisation solution for protection.

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 22.125: "Unmanned Aerial System (UAS) support in 3GPP".

[3] 3GPP TR 23.754: " Study on supporting Unmanned Aerial Systems (UAS) connectivity, Identification and tracking".

[4] 3GPP TR 23.755: "Study on application layer support for Unmanned Aerial Systems (UAS)".

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

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

The following definitions are adopted from TS 22.125 [2]:

Unmanned Aerial System (UAS)

Editor's note: The following definitions are in TS 23.754 v0.2.0 and are included for information.

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.

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).

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 Remote ID: The capability of providing Remote Identification and Tracking over 3GPP network.

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 as identified in 'FAA Remote Identification of Unmanned Aircraft System' [2].

The following definitions are adopted from TS 22.125 [5]:

Above ground level (AGL)

Unmanned Aerial System (UAS)

The following definitions are adopted from TR 23.755 [6]:

Remote Identification (Remote ID) of UAS

UAS Service Supplier (USS)

UAS Traffic Management (UTM)

UAV controller

3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

Editor's Note: Example needs to be deleted

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

Editor's Note: Example needs to be deleted

4 Overview of unmanned Aerial Systems (UAS)

The main objective of 3GPP systems is to facilitate non-3GPP entities UAS Service Supplier (USS) and/or UAS Traffic Management (UTM), which supply services to civil aviation authority (CAA), and provide UAS Remote Identification (Remote ID) services. UAS Remote ID refers to a UAS in flight provides identification and tracking information that can be received by regulatory agencies.

An Unmanned Aerial System (UAS) is composed of an Unmanned Aerial Vehicle (UAV) and a UAV controller (UAVC).

TPAE is the Third Party Authorized Entity which can monitor UAVs, access and track UAV data, and make controls to UAVs.

A UAV can be controlled by either a UAVC, TPAE, or UTM.

Clause 4 of TS 23.574 [3] provides some architectural assumptions and requirements and an overall reference architecture for the supporting UAS.

Editor's note: The UAS security aspects that are in scope of 3GPP SA3 is FFS.

Editor's note: It is FFS if a UAS authentication is applicable to UAV-C and if not how a UAV-C is considered as authenticated.

5 Key issues

Editor's Note: This clause will contain the agreed key issues

5.1 Key issue #1: UAS authentication and authorization

5.1.1 Key issue details

Each UAS consists of one UAV Controller (i.e. UAVC) and one UAV.

As stated in Architectural Assumptions of TR 23.754 [3], each UAV is assigned two types of IDs as follows, in addition to UE ID (e.g. SUPI) and Credentials used for registration in 3GPP networks:

- Civil Aviation Authority (CAA) level UAV ID assigned by USS/UTM and used for Remote Identification and Tracking.
- 3GPP UAV ID assigned by the 3GPP system and used by the 3GPP system to identify the UAV

The 3GPP Core Network is aware of the CAA-level UAV ID and the mapping between the CAA-level UAV ID and the 3GPP UAV ID [3].

To support Unmanned Aerial Systems (UAS) regarding connectivity, identification and tracking, the 3GPP system (e.g. AMF, gNB) should be aware of these UAV identities and the special nature of a drone, i.e. a potentially high and fast flying object and whether UAV or UAVC roles are authorized in the drone domain, i.e. after UAV and UAVC have been successfully authenticated and authorized, information from the UTM/USS/AF needs to be provided to the 3GPP system providing connectivity. This allows the 3GPP system to set certain policies. In case of unsuccessful Authentication and Authorization, the 3GPP system may act and de-register the UE or terminate existing PDU connections. However, the use case of a drone when not active in UAS operation performing software updates using 3GPP system needs to be also considered, in which case deregistering and termination of the existing connections may be not appropriate.

The 3GPP UAV ID is used by the UAV to access the services provided by 3GPP systems, e.g. Remote Identification. The UAV shall be authenticated to prevent illegal access to the UAS services provided by 3GPP systems. On the other hand, the 3GPP system should allow authentication of USS/UTM to prevent false USS/UTM.

Further, the 3GPP system shall also enable UTM/USS to revoke UAV authorisation and indicate to 3GPP system revoked UAVs/UAVCs.

NOTE: Authentication and Authorization by USS/UTM to access UAS services provided by 3GPP systems applies to both UAV and networked UAVC. Non-networked UAVC are not in scope of this KI.

5.1.2 Threats

If UAS authentication is not performed, unauthorized UEs/UAVs may access the UAS services provided by 3GPP and consume resources meant for authorized UEs/UAVs. It is notable that the unauthorized UEs may be a regular UE or a UAV with 3GPP ID/credentials. They may be able to access 3GPP networks using 3GPP credentials, but do not have credentials for access UAS services.

If 5GC would not be notified of UAS authentication result, 5GS may allow access UAVs in their system that are not authorized.

If the UAS authentication process is not standardized there may be costly proprietary solutions which may result in potential security risks with respect to proprietary solutions.

If 3GPP system is not capable to receive revocation of UTM/USS authorisation, UTM/USS might not be able to take appropriate measures to deal with misbehaving UAVs and they might cause accidents or become attack vectors.

A fake USS/UTM may allow unauthorized UAVs to operate.

5.1.3 Potential security requirements

A UAV or networked UAVC shall be authenticated and authorized in addition to Primary Authentication before being allowed to access UAS services provided by 3GPP systems.

The 3GPP system shall enable UAV or networked UAVC authentication and authorisation by the UTM/USS utilising the 3GPP system.

The 3GPP system shall enable revocation of UAV or networked UAVC authorisation by the UTM/USS utilising the 3GPP system.

The 3GPP system shall ensure that the USS/UTM is authorised to provide the authorisation of the UAV or networked UAVC.

5.2 Key issue #2: Pairing authorization for UAV and UAVC

5.2.1 Key issue details

Each UAS consists of one UAV Controller (i.e. UAVC) and one UAV.

It is required in TR 23.754 [3] that

- 3GPP system shall enable UTM to associate/pair the UAV and UAVC.
- Pairing is authorized by the USS/UTM and the result is made known to the PLMN
- Pairing between UAV and UAVC for the use of their connection may be at least authorized

This key issue discuss the detailed 3GPP security procedure for the pairing authorization of UAV and UAVC.

5.2.2 Threats

If pairing authorization of UAV and UAVC is not performed securely before establishment of a connection between the UAV and UAVC, an unauthorized UAVC may be able to communicate with the UAV and perform an unauthorised flight which could cause tremendous risks to the security of UAS and public safety.

If 3GPP system is not capable to receive revocation of the connectivity pairing authorisation from UTM/USS, then UTM/USS might not be able to take appropriate measures to deal with misbehaving UAVs and they might cause accidents or become attack vectors.

5.2.3 Potential security requirements

3GPP system shall support enabling authentication and authorization by the USS/UTM of a UAV and UAVC pairing before enabling a data connection between the UAV and UAVC

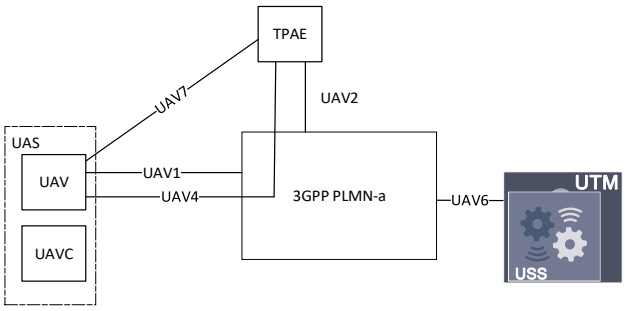
3GPP system shall provide means for the UTM/USS to revoke a UAV and UAVC pairing authorization in order to close the connection between the UAV and UAVC.

NOTE: The authorization decision for pairing a UAV and a UAVC is always done by the USS/UTM. The 3GPP system will support the USS/UTM to enforce that decision.

5.3 Key Issue #3: TPAE authentication and authorization

5.3.1 Key issue details

TPAE refers to the Third Party Authorized Entity. It has been introduced as part of the Reference Architecture in TR23.754 [3], as illustrated in the figure below.



TPAE is one component of the Remote Identification framework, where TPAE can monitor UAVs, access and track UAV data, and make controls to UAVs, overruling UAVC if necessary. TPAE may be treated as a UE, NF, or third party entity, depending on application scenarios. The access based on 3GPP systems and interfaces to the 3GPP systems, e.g. so called UAV2, UAV4, and UAV 7 are being studied in TR 23.754 [3] (UAV2 semantics are outside SA2 study, but UAV identification information is within the scope).

Since TPAE may take control of UAVs and potentially overrules UAVC, it shall be authenticated and authorized different from a normal UAVC, UAV, or UE.

5.3.2 Threats

Without authentication and authorization, potential attackers may hijack a UAV through 3GPP networks.

5.3.3 Potential security requirements

The TPAE shall be authorized and authenticated by 3GPP systems

The TPAE shall be authorized and authenticated by USS/UTM.

Editor's note: it is ffs whether authorization and authentication by USS/UTM is out of scope of 3GPP.

5.4 Key issue #4: Location information veracity and location tracking authorization

5.4.1 Key issue details

The UAV can report to USS/UTM various types of location information including absolute positioning, e.g., GNSS coordinates and/or relative positioning, such as Cell, tracking area based coordinates nearby UAVs at the particular time instance. The USS/UTM may make decisions based on the reported location information.

When reporting location information to the USS/UTM via application layer mechanisms such as Networked Remote ID, a UAV may report false location information to the USS/UTM which could results in the UTM/USS making an incorrect decision.

5.4.2 Threats

The Location Information that is reported by the UAV to the USS/UTM may be spoofed and forged by the following ways:

1. Externally, e.g. false location information derived from spoofed GNSS transmitter, spoofed neighbour Cell IDs is reported to the USS/UTM.

2. Internally, e.g., a compromised UAV reports forged Location Information regardless of received e.g., GNSS signals or neighbour Cell IDs.

3. Hybrid attack, i.e., both, externally and internally.

USS/UTM may make decisions based on the reported location information. When UAV or UAV Controller reports false location information to the USS/UTM, UEs and/or USS/UTM may make decisions that are based on falsified Location Information. For example, the UAV may deviate from an authorized flight path (e.g., unnoticed) or prevent authorities to adequately correlate a UAV under observation with its remote ID information (e.g., UAV visible in an area but not present in that area based on Remote ID USS information). Such decisions may lead to costly cyber-physical and/or kinetic attacks.

If an unauthorized entity (e.g., competitor USS/UTM) can obtain UAV location information from the 3GPP system (e.g., for a list of UAVs in a target geographic area), the attacker can use that information to mount privacy attacks on UAV and/or collect sensitive flight information.

5.4.3 Potential security requirements

3GPP system shall provide means to mitigate against UAVs or networked UAV controller location spoofing.

3GPP system shall support to authorize a USS/UTM to request UAV location information.

5.5 Key issue #5: Privacy protection of UAS identities

5.5.1 Key issue details

3GPP system will enable UAV and UAV-C to transmit identities and other potentially sensitive information (e.g., UE capability of the UAV controller, position, owner identity, owner address, owner contact details, owner certification, UAV operator identity, UAV operator license, UAV operator certification, UAV pilot identity, UAV pilot license, UAV pilot certification and flight plan). The 3GPP system will enable UAV or UAV controller to preserve the privacy of UAS identities when transmitted over broadcast or towards USS/UTM.

TR 22.125 [2] in Clause 5.1 General has the following requirements:

[R-5.1-002] The 3GPP system shall be able to provide UTM with the identity/identities of a UAS.

[R-5.1-003] The 3GPP system shall enable a UAS to send UTM the UAV data which can contain: unique identity (this may be a 3GPP identity), UE capability of the UAV, make & model, serial number, take-off weight, position, owner identity, owner address, owner contact details, owner certification, take-off location, mission type, route data, operating status.

[R-5.1-004] The 3GPP system shall enable a UAS to send UTM the UAV controller data which can contain: unique identity (this may be a 3GPP identity), UE capability of the UAV controller, position, owner identity, owner address, owner contact details, owner certification, UAV operator identity, UAV operator license, UAV operator certification, UAV pilot identity, UAV pilot license, UAV pilot certification and flight plan.

[R-5.1-007] Based on regulations and security protection, the 3GPP system shall enable a UAS to send UTM the identifiers which can be: IMEI, MSISDN, or IMSI, or IP address.

[R-5.1-008] The 3GPP system shall enable a UE in a UAS to send the following identifiers to a UTM: IMEI, MSISDN, or IMSI, or IP address

TS 22.125 [2] in Clause 5.2.2, Decentralized UAS traffic management, has the following requirement:

[R-5.2.2-003] The 3GPP system shall enable UAV to preserve the privacy of the owner of the UAV, UAV pilot, and the UAV operator in its broadcast of identity information.

TS 22.125 [2] in Clause 5.4, Security, has the following requirement:

[R-5.4-005] The 3GPP system shall support confidentiality protection of identities related to the UAS and personally identifiable information.

With support of a 3GPP system studied and reported in TR23.754 [x1], the following identities are being defined with respect to UAS Remote Identification:

- CAA-level UAV ID assigned by USS/UTM and used for Remote Identification and Tracking.
- 3GPP UAV ID assigned and used by the 3GPP system to identify the UAV

This key issue studies whether security solutions for 3GPP systems are required to protect the CAA-Level UAV ID, 3GPP UAV ID, and/or other information (e.g. locations etc.) for privacy.

5.5.2 Threats

If an attacker can glean the UAV and UAV-C identities and other information while transmitted, such attacker can maliciously employ the knowledge of UAV and UAV-C identities to mount privacy attacks on UAV and UAV-C (e.g., tracking attack). For example, an attacker may be able to collect and analyze flight information of a particular UAS operations revealing sensitive business practices, such as the flight profile of an individual UAS over time (see FAA's proposed rule on Remote Identification of Unmanned Aircraft Systems [5]).

5.5.3 Potential security requirements

The 3GPP system shall provide means for mitigating linkability and trackability attacks on UAV and UAV controller identities during communications with USS/UTM.

The 3GPP system shall provide means for mitigating linkability and trackability attacks on UAV and UAV controller identities during C2 communications.

Editor's Note: This requirement may not be possible to solve in all cases – it may be necessary to limit its scope.

The 3GPP system shall enable UAV and UAV controller to preserve the privacy of UAS owner/operator/pilot, including associated PII.

5.6 Key issue #6: Security protection of information in remote identification and between UAV/UAVC and UTM/USS

5.6.1 Key issue details

In TR 23.754 [3], UAV remote identification (Remote ID) procedure is discussed. In this procedure, the UAVs send the messages with flight information (e.g. height, direction, speed, time of flight, etc.) to the receiving party (i.e. UTM/USS, a TPAE or another UAV). The information may be sent in broadcast or unicast. Upon receiving the UAV flight information, a receiving party verifies the validity of the Flight Information, and may use such information for e.g. collision avoidance.

Apart from protecting the Remote ID between UAS and UTM/USS, 3GPP TS 22.125 [2] gives several security-related requirements for protecting other exchanged information between UAS and UTM/USS (e.g., UE capability of the UAV controller, position, owner identity, owner address, owner contact details, owner certification, UAV operator identity, UAV operator license, UAV operator certification, UAV pilot identity, UAV pilot license, UAV pilot certification and flight plan) and user identity. TS 22.125 [2] in Clause 5.4 specifics the security requirement to protect data transport between UAS and UTM (R-5.4-001), and TS 22.125 [2] in Clause 5.1 has the requirements (R-5.1-002 to R-5.1-004, R-5.1-007 to R-5.1-008 and R-5.1-017) of UAS identity protection.

To sum up, 3GPP system shall be able to secure the information exchange (e.g. flight information, user identity, etc) between UAV/UAVC and the receiving party (i.e. UTM/USS, TPAE and other UAV) within the scope of 3GPP, this involves the Remote ID and general information exchanging procedures.

5.6.2 Threats

If the messages with flight information are modified or replayed by attackers, the received party (i.e. a TPAE or UTM/USS) may be spoofed to believe the UAV appear to perform other than what they actually did. In the worst case, a collision may happen between different UAVs.

If an attacker can glean and modify the UAV and UAV-C identities and other information during its transport from the 3GPP system to the UTM/USS entity, such attacker can maliciously use the knowledge of and the ability to modify UAV and UAV-C identities to mount attacks on UAV and UAV-C identities' confidentiality and integrity (e.g., subscription fraud, impersonation attacks, and hiding problematic/misbehaving UAS).

An attack on integrity or confidentiality of the information exchanged between UAV or UAV-C and USS/UTM may lead to catastrophic loss of overall UAS integrity (e.g., with potential risks to public safety).

5.6.3 Potential security requirements

The 5G System shall provide the means for the USS/UTM to transport security information to the UE to secure communication between UAV and TPAE/UTM/USS.

NOTE: UAS-specific and general exchanged information do not include C2.

5.7 Key issue #7: Security of command and control (C2) communication

5.7.1 Key issue details

The TS 22.125 [2] describes about the UAS reference model where an UAS is composed of one UAV controller and one UAV. A UAV can be controlled by a UAV controller connected via the 3GPP mobile network to perform the desired UAV operations through the command and control (C2) signaling which is an application data. Further TR 23.754 [3] clarifies in the architectural assumptions that Connectivity for Command and control of a UAV may be between the UAV and, mutually exclusively, an UAV controller (UAV-C), or a Third Party Authorized Entity (TPAE), or the UAS Service Supplier/UAS Traffic Management (USS/UTM). Therefore, C2 to a UAV may be either over UAV3 or, UAV4 or UAV9 interface. The Command and control traffic exchanged with UAV over various interfaces if not protected (Confidentiality, and integrity) will give way for the attackers to take control of the UAV operations leading to more critical outcomes such as hijacking of UAVs, tracking of UAVs, potential misoperation and accidents. The protection of C2 traffic over the UAV radio link alone may be insufficient since the peer UAV controller may be connected via a different PLMN or a different access technology, using a different security policy for User Plane traffic (e.g., with no integrity and/or no confidentiality protection). In general, the security of the UAV controller connection may be outside the control of the MNO who provides the service to the UAV.

5.7.2 Threats

The lack of C2 communication security between UAV and other parties such as UAV-C, TPAE and USS/UTM over UAV3, UAV4 and UAV9 may let the attackers to eavesdrop and control the UAV operations thereby leading to UAV hijack and misoperations.

As the UAV controller could be connected via a different PLMN or using a different access technology with a different security policy (e.g., with no integrity and/or no confidentiality protection) the C2 communication security with the UAV may be compromised via the UAV controller connection.

5.7.3 Potential security requirements

The 3GPP system shall provide means for the USS/UTM to transport security information to the UE to secure C2 Communication as part of the UAS Security.

NOTE: The method and security information used to establish C2 security and how to apply C2 Security is up to USS/UTM and is outside the scope of 3GPP.

Editor's Note: This below provides a generic set of headings for a new key issue and need to be deleted before the TR goes for approval

5.X Key issue #X: <Key issue name>

5.X.1 Key issue details

5.X.2 Threats

5.X.3 Potential security requirements

6 Proposed solutions

Editor's Note: This clause will contain the proposed solutions

6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of solutions to key issues

Solutions	KI#1	KI#2	KI#3	KI#4	KI#5	KI#6	KI#7	
#1: UAS authentication and authorization	x							
#2: UAS authentication and authorization using User Plane	x							
#3: UAV authentication and authorization by USS/UTM with AMF as authenticator	x							
#4: UAV authentication and authorization using EAP-based PDU secondary authentication	x							
#5: UAV authentication and authorization using API-based PDU secondary authentication	x	x				x	x	
#6: Obtaining UAV location information from the PLMN				x				
#7: UAS authentication, authorization and security aspects	x					x		
#8: Using 5G location result for location information verification				x				
#9: UAS enabled authentication	x							
#10: Authentication and authorisation of UAVs	x							
#11: UAV and UAVC pairing authorization through bound IDs		x						
#12: UAV location privacy protection	x			x	x			
#13: Authorisation of UAV/UAVC when connected to EPS	x	x						

#14: Authorisation of UAV/UAVC pairing when connected to 5GS		x						
#15: UAV and UAV-C Pairing Authorization and Security Aspects		x					x	
#16: Preventing malicious revocation from unauthorised UTM/USS	x							

6.1 Solution #1: UAS authentication and authorization

6.1.1 Solution overview

This solution address the key issue #1.

This solution assumes each UAV or UAVC is provisioned with a PLMN UE ID (SUPI) and the corresponding credential so that it can be authenticated (primary authentication) by the PLMN as a normal UE. In addition, UAV or UAVC is provisioned with a UAS ID and corresponding credentials to perform UAS authentication and authorization (UAA) with USS/UTM.

The UAA is mandatory for UAA or UAVC and is based on EAP framework, where AMF is taking the role of the transparent Authenticator.

6.1.2 Solution details

6.1.2.1 Registration

The call flow of this solution is shown in the figure below.

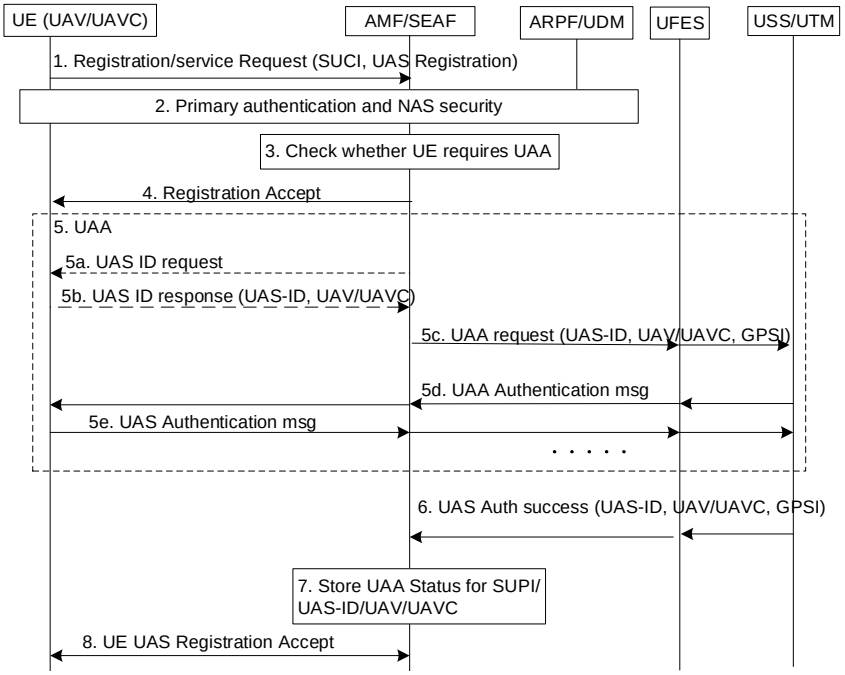


Figure 6.1.2.1-1: UAA procedure

1. UAV (or UAVC) sends registration request to AMF. It may indicate that this is a registration for UAS.

NOTE: a new IE or an extension of an existing IE can be used to indicate UAA is requested. The IE can be defined in stage 3 and in coordination with CT.

2. AMF initiates Primary authentication as a normal UE

3. After successful Primary authentication, AMF checks whether UAV (or UAVC) requires UAA. This may be based on the subscription information retrieved from UDM in step 2

4. AMF returns a Registration Accept message to the UAV and indicates that UAA is pending.

5. UAA starts with EAP message exchanges.

a. AMF may optionally request UAS ID from UE.

b. UAV (or UAVC) responses with UAS ID. It may indicate whether this is a UAV or UAVC.

c. AMF sends UAA requests to UFES (as defined in TR 23.754 [3]) with UAS-ID and UAV or UAVC indicator in the EAP message. In addition, UAA request contains GPSI for USS/UTM to identify the UAV. GPSI shall be bound to UAS-ID. UFES locates the corresponding USS and forwards the UAA requests to it.

d. USS/UTM response with EAP messages to AMF through UFES accordingly

e. EAP messages may continue based on the EAP method used.

f. …

Note: the EAP authentication method used by UTM is out of scope of 3GPP

6. Based on the EAP authentication outcome, USS/UTM sends the results to AMF through UFES. If successful, USS/UTM sends the EAP-Success message, together with UAV/UAVC's GPSI and UAS-ID that can uniquely identity the UAV/UAVC.

7. AMF stores the results, together with SUPI (converted from GPSI), UAS-ID, and UAV/UAVC indicator

8. AMF triggers the UE Configuration Update procedure. The message AMF sent to UE includes the UAS-ID and may include an indication it is for a UAV (or UAVC), if needed.

6.1.2.2 Revocation

USS/UTM may trigger revocation of UAA at any time. The call flow is shown in the figure 6.1.2.2-1.

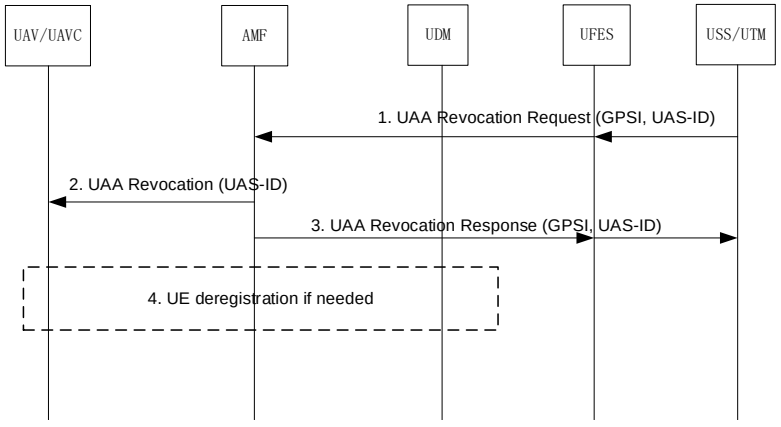


Figure 6.1.2.2-1: UAA revocation procedure

1. The USS/UTM sends the UAA revocation request to AMF through UFES to revoke the UAS service for a UAV. The UAV is identified by the GPSI and UAS-ID in the UAA revocation Request.

NOTE: UFES is an NF interfacing USS/UTM and it can locate AMF serving the UAV.

2. The AMF may inform UAV with the UAA revocation message.

3. The AMF responses USS that the UAV's authentication and authorization is revocated.

4. The network may deregister the UAV if needed, as per current procedure.

6.1.3 Solution evaluation

This solution addresses the key issue #1 (the fourth requirement for the fake USS/UTM has not been addressed).

In this solution, each UAV is assumed to be provisioned with UE ID (i.e. SUPI by PLMN) as well as UAS ID (by USS/UTM), together with corresponding credentials for authentication. The UAS authentication and authorization (UAA) with USS/UTM is performed after UAV is authenticated with the network (using UE ID).

This solution supports multiple UAA methods to meet potential different authentication requirements from USS/UTM. EAP framework can be used to carry the UAA messages.

This solution supports revocation triggered by USS/UTM at any time.

6.2 Solution #2: UAS authentication and authorization using User Plane

6.2.1 Solution overview

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

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

The solution allows the execution of A&A procedure between UAV and USS/UTM where 3GPP provides communication between UAV and USS/UTM. For this communication, first the UAV needs to execute primary authentication, so the UAV and 3GPP execute mutual authentication. Then when the UAV wants to get UAV related service, 3GPP system allows the UAV to communicate with the UAS AF located in the inside of the operator network. The UAS AF and the USS/UTM communicates via NEF framework which requires mutual authentication. As a result, there is a hop-by-hop mutual authentication between UAV and USS/UTM during UUAA procedure. The A&A protocol is out of 3GPP scope and this protocol may provide additional mutual authentication between UAV and USS/UTM using their credentials which are out of 3GPP scope.

Also, this solution includes an authorization revocation mechanism that allows the authorization revocation triggered by USS/UTM.

6.2.2 Solution details

The authentication and authorization procedures for 5GS and EPS are presented in clause 6.2.2.1 and 6.2.2.2, respectively.

6.2.2.1 Procedure for 5GS

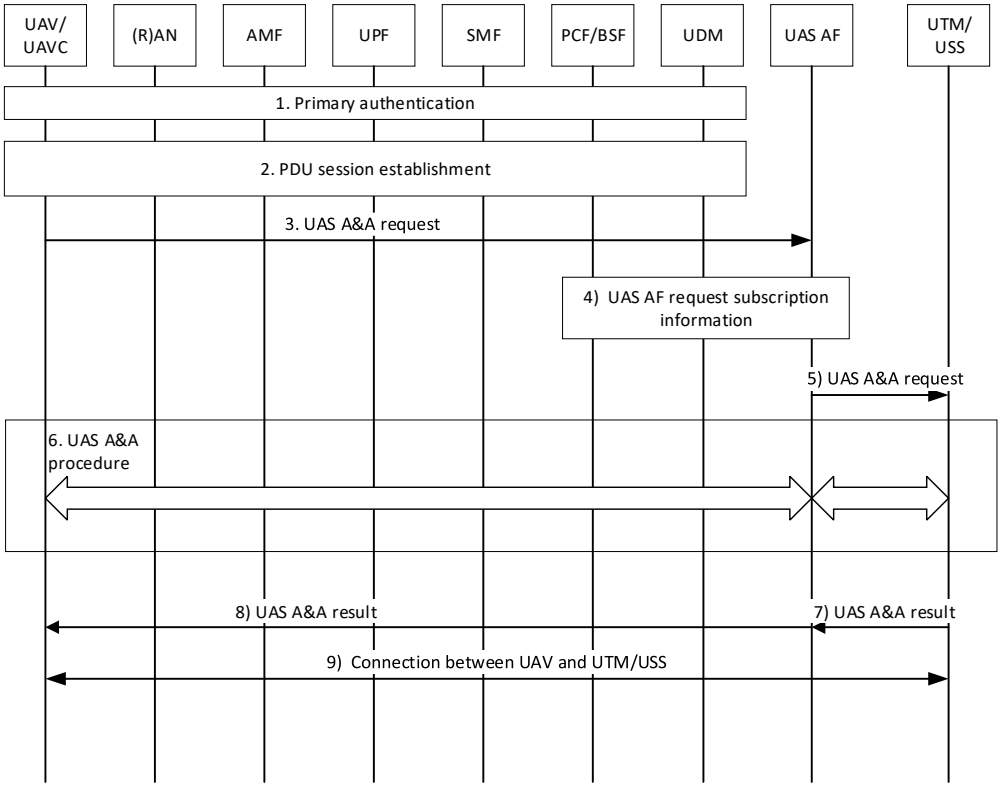


Figure 6.2.2.1-1: UAV Authentication and Authorization procedure for 5GS

1. Primary authentication is performed.

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

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

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

3. UAV/ UAVC sends the request for authentication and authorization to the UAS AF over the user plane, e.g. including UAV/UAVC identity, USS/UTM identity (if available), and application level information, transparent to 3GPP and out of 3GPP scope, to be used by the USS/UTM when authenticating the UAV.

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

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

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

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

UAV/UAVC specific information received in the UAS A&A request. For the communication between UAS AF and USS/UTM, the NEF or the Common API framework (CAPIF) is used.

6. An authentication and authorization procedure is executed between UAV/UAVC and USS/UTM. UAS AF relays the messages in this A&A procedure providing API's, which use well-known web security mechanisms such as HTTPS, for the UAV-application and USS/UTM. USS/UTM considers the combined information from the UAV/UAVC and from the mobile network operator of the UAV/UAVC while performing the procedure. Note that if the information sent to the USS/UTM before this step is enough for the authentication&authorization procedure, there may be no need for extra message exchange between the UAV/UAVC and USS/UTM.

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

7. USS/UTM sends UAS A&A result to UAS AF.

   If the A&A result is successful, then USS/UTM may provide application specific information to be used for secure communication establishment between UAV and UTM/USS. This information is transparent to the network and the content is out of 3GPP scope. The network relays this information from the UTM/USS to the UAV.

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

8. The UAS AF sends the response to the UAV.

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

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

NOTE 5: This solution does not enable/support authorization of UAV and UAVC pairing.

6.2.2.2 Procedure for EPS

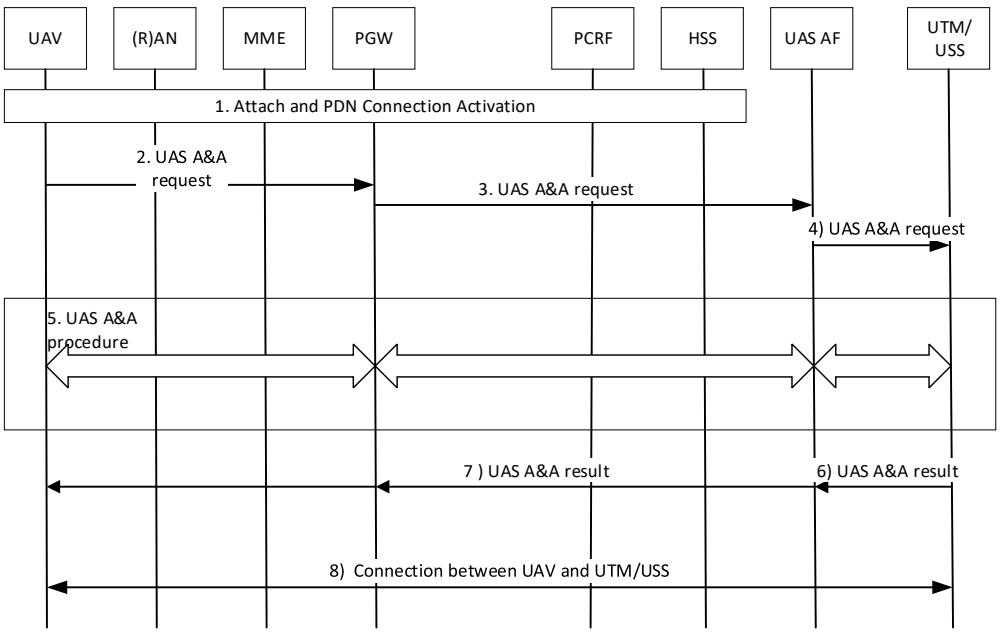


Figure 6.2.2.Y-1: UAV Authentication and Authorization procedure for EPS

1. Attach and a PDN connection activation procedures are performed. As the UAV has a subscription indicating UAV capability the PCRF generates a PCC rule indicating UAV application and header enrichment policy.

2. UAV sends UAS A&A request to the UAS AF.

3. PGW detects the UAV application traffic and adds UAV subscription information.

NOTE: In case of end-to-end security between UAV and UAS AF, to enable the PGW to add UAV subscription information, a HTTP(S) proxy functionality in the PGW is integrated under the assumption that TLS is used for end-to-end security. The certificate of the UAS-AF needs to be provisioned to the PGW. The PGW terminates TLS for HTTPS-requests towards to the UAS-AF and then apply header-enrichment.

4. UAS AF checks if the UAV has a valid aerial subscription based on the subscription information received from the PGW.

If the check is successful, the UAS AF based on the UTM/USS identity, looks up the corresponding UTM/USS URL and triggers a request towards the UTM/USS. If the check is unsuccessful a response is sent to the UAV rejecting the request. The UAS AF can include information to the UTM/USS needed for further interaction between UTM/USS using network APIs and EPS regarding the PDU session.

5. UTM/USS performs authentication and authorization steps which are transparent to the network. In this communication, the UAS AF and PGW relay the traffic between UAV and UTM/USS.

6. If the A&A in step 5 is successful, UTM/USS triggers a accept response to UAS AF acknowledging the request including an application specific information such as a security context to be used in the establishment of secure connection between UAV and UTM/USS. The transfer of this information is transparent to the network and the content of it is out of 3GPP scope.

If the A&A is un-successful, a response is sent to the UAV rejecting the request.

7. The UAS AF sends the response to the UAV.

8. UAV triggers a set-up of a secure connection to UTM/USS e.g. using the information received in step 7.

6.2.2.3 Authorization revocation mechanism

When the USS/UTM wants to trigger authorization revocation, it calls the NEF API (AsSessionWithQoS) used to activate, modify, and revoke policies for specific data flows on a specific PDU-session/PDN-connection. UAS AF provides related information needed by the USS/UTM to call that API, during the authentication and authorization procedure.

During the authentication and authorization procedure, UAS AF provides the UE-IP of the UAV to the USS/UTM. After successful authentication and authorization by the USS/UTM, the USS/UTM calls AsSessionWithQoS to activate the authorized policies for the PDU-session and then waits for a notification on that they have been successfully enforced. Then the USS/UTM sends the A&A result back to the UAS-AF which will forward the result to the UAV.

6.2.3 Solution evaluation

This solution fully addresses key issue #1 having no effect on the current NAS procedures and UAV UE proposing a UP solution.

This solution provides a user plane solution while TR 23.754 [3] concludes on using control plane based UUAA procedures.

This solution requires a new function (UAS AF) that requires updates on AMF and PCF for the subscription information requests.

It uses web-based interface for the communication between UAS AF and USS/ UTM.

6.3 Solution #3: UAV authentication and authorization by USS/UTM during Registration

6.3.1 Solution overview

This solution addresses Key Issue#1 "UAS Authentication and Authorization".

This solution is applicable to 5GS and to both UAV and networked UAV-C.

This solution enables an authentication and authorization (A&A) with a USS/UTM during registration after primary authentication successful completion in a procedure similar to Network Slice Specific Authentication and Authorization (NSSAA). An API-based authentication procedure is triggered by AMF following a Registration procedure based on the UE subscription and capabilities information. The procedure for authentication and authorization (A&A) by the USS/UTM is performed using non-3GPP credentials (e.g., CAA-level UAV ID, certificate). The AMF forwards transparently the authentication messages between the UAV and the USS/UTM. The solution proposes an A&A Proxy function to be used for A&A communication with USS/UTM. This A&A Proxy function may be integrated in the UAS-NF as defined in TR 23.754[3] clause 8.

The USS/UTM may initiate UAV authorization revocation at any time after successful completion of authorization procedure.

6.3.2 Solution details

6.3.2.1 UAV authentication and authorization by USS/UTM

The procedure for UAV Authentication and Authorization by USS/UTM during registration, is depicted in Figure 6.3.2.1-1. The same procedure may be used with a networked UAV-C.

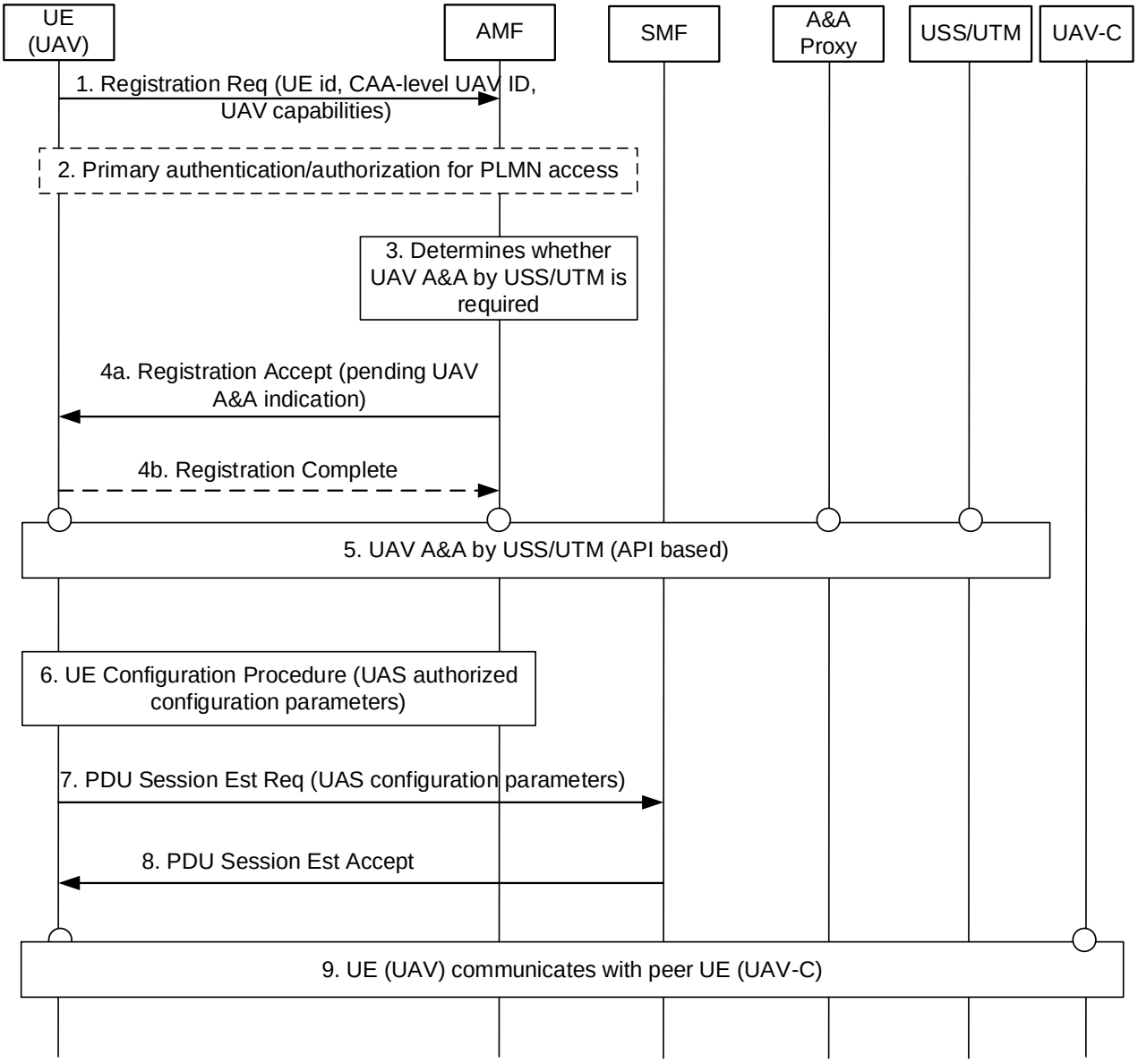


Figure 6.3.2.1-1: Procedure for UAV authentication and authorization with USS/UTM during registration

Pre-condition: UAV is configured with a long-term UAV ID (e.g., serial number, CAA registration id) and credentials used for authentication by USS/UTM. The UAV ID and credentials are obtained by means outside of 3GPP scope

1. The UE sends a Registration Request message including its UE id, a UAV id and UAV communications capabilities. UE may provide a USS/UTM address if available.

NOTE 1: If the UAV id is subject to privacy protection, existing partial cyphering mechanisms may be used to protect it during initial Registration transmission.

2. If the UE is not already authenticated by the network, a primary authentication procedure is performed.

3. The AMF determines whether a UAV A&A by USS/UTM is required based on:

- Subscription information (i.e., whether the UE is authorized for UAS operations)

- If the UAV is undergoing A&A by USS/UTM procedure or UAV has previously performed such procedure succesfully and the authorization was allowed and still valid.

4. AMF sends in the Registration Accept message a pending UAV A&A indication. UE refrains from establishing PDU Session dedicated to UAS communications until the successful completion of the following A&A steps. The Registration Accept message may include some other configuration information such as allowed UAS communication modes/types (e.g., network assisted, direct). The UE sends a Registration Complete if this is an initial Registration.

5. AMF triggers an API-based UAV A&A by USS/UTM procedure. UE is authenticated using UAV credentials (e.g., CAA-level UAV ID, certificate). During the procedure, the AMF provides the USS/UTM with a 3GPP UAV ID (e.g., GPSI as External id) and AMF may receive a CAA-level UAV id (e.g., a temporary Session id) from USS/UTM. The AMF stores the CAA-level UAV id in the UE context. The AMF may use the CAA-level UAV id to determine whether to perform UAV A&A as described in step 2. The AMF provides the CAA-level UAV id and to the UE in the following step.

NOTE 2: It is assumed that the AMF may communicate with the USS/UTM using an A&A proxy function (similar to NSSAAF). This proxy function provides USS/UTM discovery/address resolution, authentication messages routing and protocol translation capabilities. Authentication of USS/UTM is supported by the A&A proxy by means of provisioned aviation domain certificates. USS/UTM address may be obtained from a trusted resolution function that can resolve the USS/UTM address from the CAA-level UAV ID (if USS/UTM address was not provided by the UE in step 1).

6. Upon successful UAV A&A by USS/UTM, AMF initiates the UE Configuration Update procedure to deliver authorized UAS Configuration parameters to the UE. The UAS Configuration may include the following parameters to be used for UAS communication setup: the CAA-level UAV ID, S-NSSAI/DNN. The CAA-level UAV ID is used for remote or broadcast Remote ID.

7. The UE establishes a PDU Session using authorized UAS parameters as provided in step 6 (e.g., CAA-level UAV ID)

8. The UE receives a PDU Session Establishment Accept message authorizing UAS communications.

9. The UE exchanges UAS traffic with peer UAV-C.

NOTE 3: PDU Session establishment and UAS communications steps above may be subject to additional pairing with UAV-C authorization. Additional details for pairing authorization are assumed to be covered in solutions for KI#2

6.3.2.2 USS/UTM triggered UAV authorization revocation

The procedure for UAV authorization revocation by USS/UTM is depicted in Figure 6.3.2.2-1.

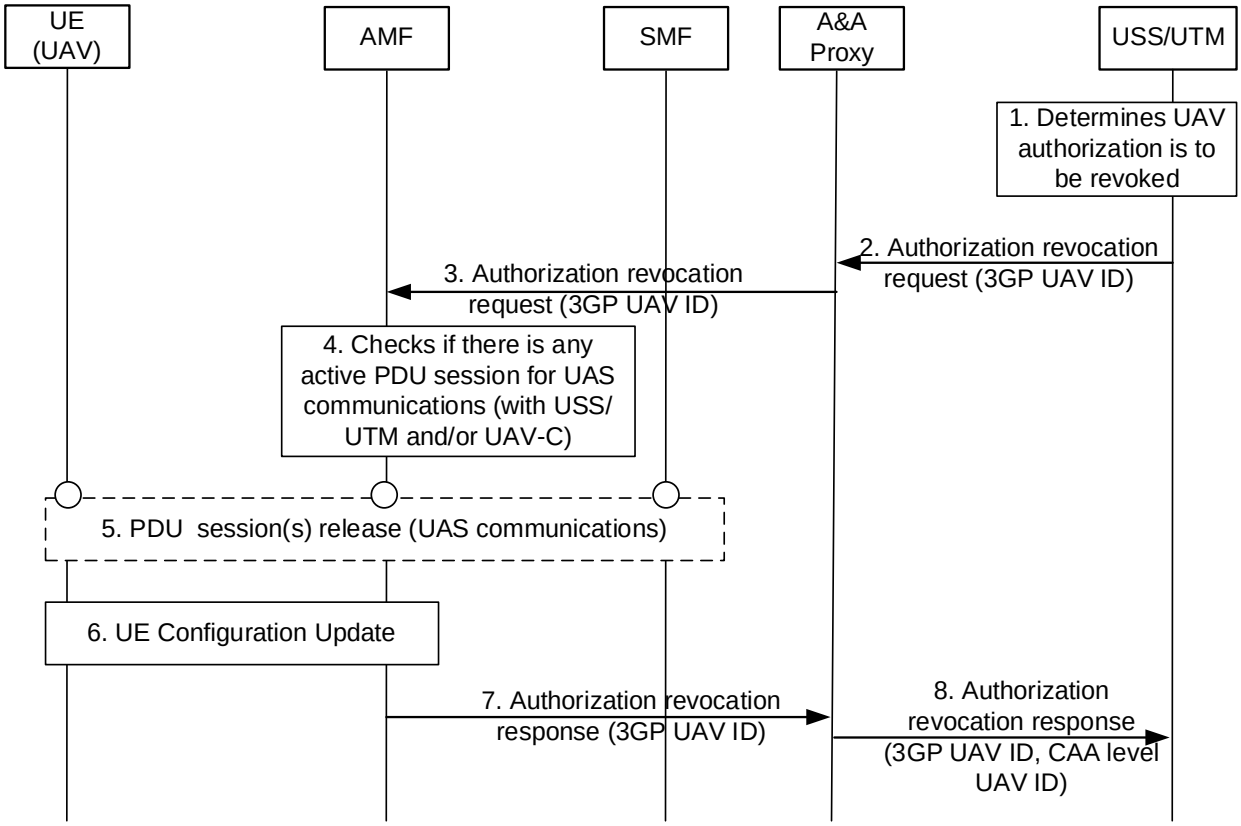


Figure 6.3.2.2-1: Procedure for USS/UTM triggered UAV authorization revocation

Pre-condition: UAV has been previously authorized by USS/UTM according to procedure 6.3.2.1.

1. The USS/UTM determines that the UAV authorization is to be revoked.

2. The USS/UTM sends an Authorization revocation request to the A&A Proxy providing the 3GPP UAV ID of the target UAV.

3. The Proxy A&A determines the AMF serving the UAV by requesting UDM providing the 3GPP UAV ID and forwards the request to the AMF.

4. The AMF checks if there are any active PDU session used for UAS communications (used with USS/UTM and/or UAV-C).

5. [Conditional] If above check is positive, the AMF initiates a PDU session release procedure for all applicable PDU sessions.

6. The AMF initiates a UCU procedure to revoke authorization information that was stored in the UE based on procedure 6.3.2.1 or initiate a DeRegistration procedure indicating the cause of deregistration.

7. The AMF sends an Authorization revocation response to the A&A Proxy confirming revocation of UAV authorization.

8. The A&A Proxy forwards the Authorization revocation response to the USS/UTM providing the 3GPP UAV ID and CAA-level UAV ID confirming revocation of authorization for the specified UAV.

6.3.3 Solution evaluation

This solution is aligned with TR 23.754 [3] conclusions for UAV authentication and authorization by USS/UTM (UUAA) during Registration, including the usage of a generic (API based) procedure using a UAS NF.

This solution fully addresses the requirements of Key Issue #1:

- The solution uses a generic (i.e., API based) procedure for UUAA during Registration via a Proxy A&A (UAS NF). The UE includes its CAA-level UAV ID to register for UAS services. After a successful primary authentication, the AMF triggers a UUAA if the UE has a valid Aerial subscription and if there is no UUAA ongoing or a valid result from a successful prior UUAA run. The AMF triggers UUAA after sending a Registration Accept message indicating a pending UUAA. The authentication method and content of authentication message used for UUAA are not in 3GPP scope.

- The solution enables the revocation of UAV authorization by the USS/UTM. The revocation request is received by the UAS NF which notifies the AMF. AMF may trigger a PDU Session release for the relevant PDU Sessions (used for communication USS/UTM and/or for C2 communications) and/or a DeRegistration procedure.

- Authentication of USS/UTM is handled by the Proxy A&A function by means of provisioned aviation domain certificates. USS/UTM address may be obtained from UE or from a trusted resolution function which provides a USS/UTM address based on a CAA-level UAV ID.

API based procedure introduces a new mechanism compared to existing EAP framework.

NOTE 1: Usage of API based is used to address an explicit requirement from the UTM community

NOTE 2: How and whether to protect the transparent containers used for UAV-USS communication during UUAA will be determined during the normative phase.

NOTE 3: IETF/3GPP protocols are readily available for EAP based mechanism to protect the transparent containers.

6.4 Solution #4: UAV authentication and authorization using EAP-based PDU secondary authentication

6.4.1 Solution overview

This solution addresses Key Issue#1 "UAS Authentication and Authorization".

This solution is applicable to 5GS and EPS for both UAV and networked UAV-C.

This solution enables a secondary authentication with a USS/UTM, reusing existing mechanisms defined for the PDU secondary authentication by an external DN-AAA procedure. An EAP-based secondary authentication is triggered by SMF during a PDU Session establishment procedure based on the UE subscription information and local policies. The authentication and authorization (A&A) by the USS/UTM procedure is performed using non-3GPP credentials (e.g., CAA-level UAV ID, certificate). The SMF acts as the EAP authenticator while the USS/UTM acts as the DN-AAA server. The same procedure can be supported in EPC by UE providing the UAV ID in a PCO and with the PGWc enhanced to support PDU secondary authentication by a DN-AAA feature (as per solutions in TR 23.754).

Editor's note: Support for equivalent to PDU Secondary authentication by DN-AAA in EPS is FFS

NOTE: for simplicity, only the non-roaming case is represented in this solution. Home Routed scenario is also supported using similar principles as for the PDU secondary authentication by external DN-AAA (i.e., V-SMF acting as a proxy for H-SMF acting as the authenticator).

The USS/UTM may initiate UAV authorization revocation at any time after successful completion of authorization procedure.

6.4.2 Solution details

6.4.2.1 UAV authentication and authorization by USS/UTM

The procedure for UAV A&A by USS/UTM based on PDU secondary authentication is depicted in Figure 6.4.2.1-1. The same procedure may be used with a networked UAV-C.

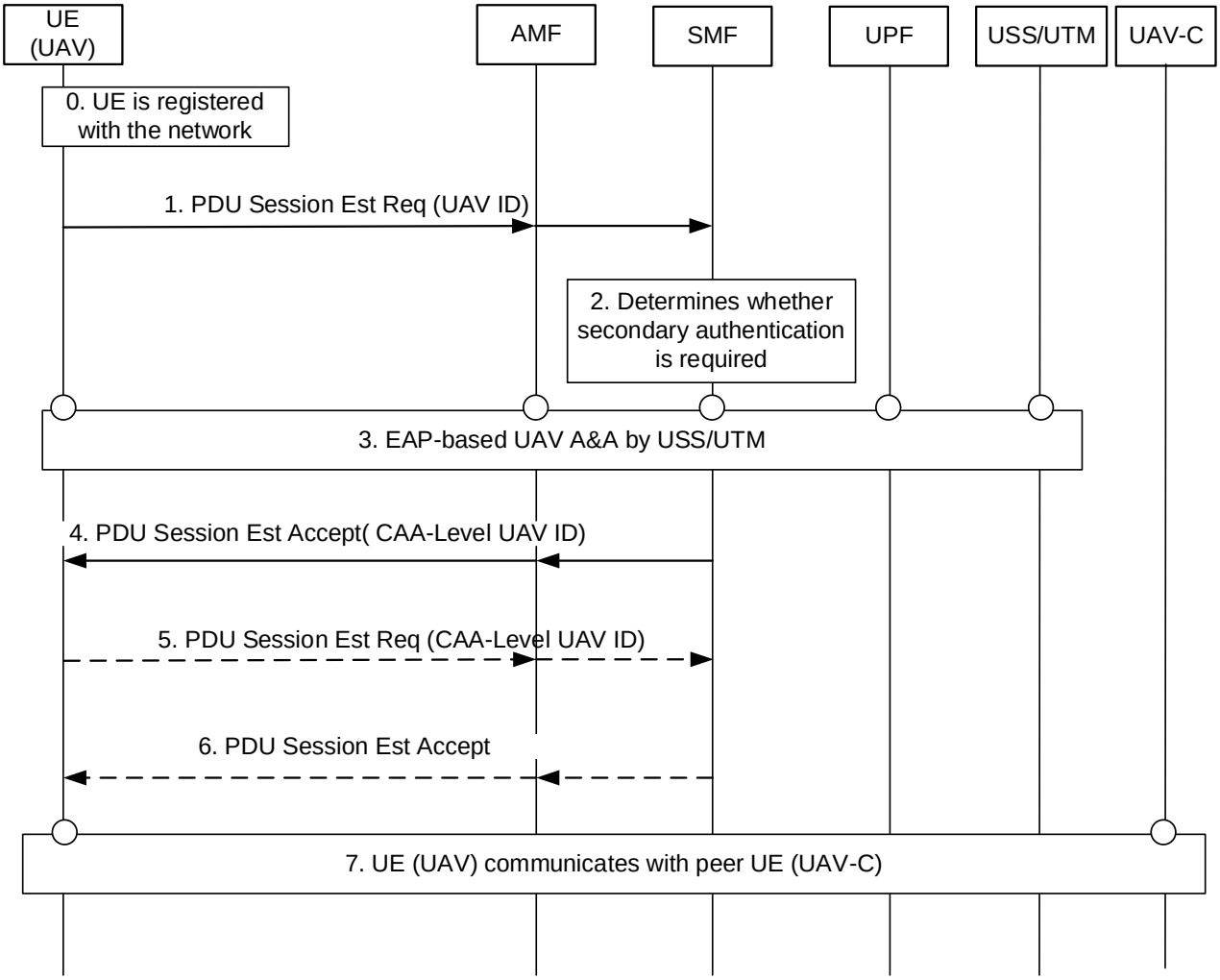


Figure 6.4.2.1-1: Procedure for UAV authentication and authorization with USS/UTM PDU Session establishment

0. The UE has successfully completed a primary authentication and is registered with the network.

1. UE sends a PDU session establishment request message that may include the following parameters: a long-term UAV ID (CAA-level UAV ID) that is communicated to the USS/UTM. The UE may also provide a USS/UTM address. AMF sends corresponding request to SMF.

NOTE 1: It is assumed the UE has obtained prior to this procedure the CAA-level UAV ID from a CAA and has been configured with a USS/UTM address by means outside of 3GPP scope

2. The SMF determines whether the UE is allowed for UAS operations based on subscription information and local policies.

3. The SMF triggers an EAP-based authentication procedure towards the USS/UTM. SMF resolves the address of the USS/UTM based on provided CAA-level UAV ID or USS/UTM address (if provided). During the procedure, the SMF provides the USS/UTM with a 3GPP UAV ID (e.g., GPSI as External id) and receives from the USS/UTM a new assigned CAA-level UAV ID (e.g., a temporary Session id) upon successful authentication and authorization.

Editor's note: details of the authentication of the USS/UTM (or its address provided by the UE) by the network are FFS

4. Upon successful authorization by USS/UTM, the SMF sends a PDU session establishment accept message that includes the new CAA-level UAV ID. The SMF provides the USS/UTM with IP address allocated for the PDU Session as specified for PDU secondary authentication by an external DN-AAA procedure (as per TS 23.502 clause 4.3.2.3).The SMF maintains the session with the USS/UTM for further updates of the PDU session that may be triggered by the USS/UTM (e.g., UAV authorization revocation triggered by USS/UTM as described in 6.3.2.2).

5. The UE may additionally establish a separate PDU Session dedicated for UAS communications. A separate PDU session is necessary if a separate DNN from the one used to communicate with USS/UTM is used for communication with a UAV-C (e.g., while the first PDU session is being used for network Remote ID and tracking functionality). The UE provides the CAA-level UAV ID obtained from successful authorization by USS/UTM.

6. The UE receives a PDU Session Establishment Accept message authorizing UAS communications.

NOTE 2: Additional details for pairing authorization performed over first or second PDU Session are assumed to be covered in solutions for KI#2

7. The UE exchanges UAS traffic with peer UAV-C.

6.4.2.2 USS/UTM triggered UAV authorization revocation

Pre-condition: UAV has been previously authorized by USS/UTM according to procedure 6.4.2.1. The SMF serving the UAV for UAS communications is maintaining a session with the USS/UTM.

The procedure for USS/UTM triggered authorization revocation is similar to authorization revocation by DN-AAA server for a PDU session subject to secondary authentication and authorization by a DN-AAA server.

The USS/UTM may decide to revoke the authorization for a PDU session used for UAS communications. The USS/UTM sends an authorization revocation request message to the SMF providing the 3GPP UAV ID and the IP address of the UE allocated to the PDU session.

The SMF releases the PDU session and sends an authorization revocation response to the USS/UTM message providing the 3GPP UAV ID and CAA level UAV ID for the specified UAV.

6.4.3 Solution evaluation

TBD

6.5 Solution #5: UAV authentication and authorization and pairing authorization using API-based PDU secondary authentication

6.5.1 Solution overview

This solution addresses the following key issues:

- Key Issue#1 "UAS Authentication and Authorization".

- Key Issue#2 "Pairing authorization for UAV and UAVC".

- Key Issue#6 "Security protection of information in remote identification and between UAV/UAVC and UTM/USS".

- Key Issue#7 "Security of command and control (C2) communication".

This solution is applicable to 5GS and EPS for both UAV and networked UAV-C.

This solution enables a secondary authentication with a USS/UTM reusing the high-level procedure defined for the PDU secondary authentication by an external DN-AAA. An API-based secondary authentication is triggered by SMF using a Proxy A&A function during a PDU Session establishment procedure, based on the UE subscription information and local policies. This Proxy A&A function may be integrated in the UAS-NF as defined in TR 23.754[3] clause 8. The authentication and authorization (A&A) by the USS/UTM procedure is performed using non-3GPP credentials (e.g., CAA-level UAV ID, certificate). Such an API based authentication enhancement is proposed to provide a broader support for DN-AAA such as USS/UTM that may not support EAP/Diameter authentication protocol.

NOTE: for simplicity, only the non-roaming case is represented in this solution. Home Routed scenario is also supported using similar principles as for the PDU secondary authentication by external DN-AAA (i.e., V-SMF acting as a proxy for H-SMF acting as the authenticator).

The USS/UTM may initiate UAV authorization revocation at any time after successful completion of authorization procedure.

6.5.2 Solution details

6.5.2.1 UAV authentication and authorization by USS/UTM

The procedure for UAV A&A by UTM using API-based PDU secondary authentication is depicted in Figure 6.5.2.1-1. The same procedure may be used with a networked UAV-C.

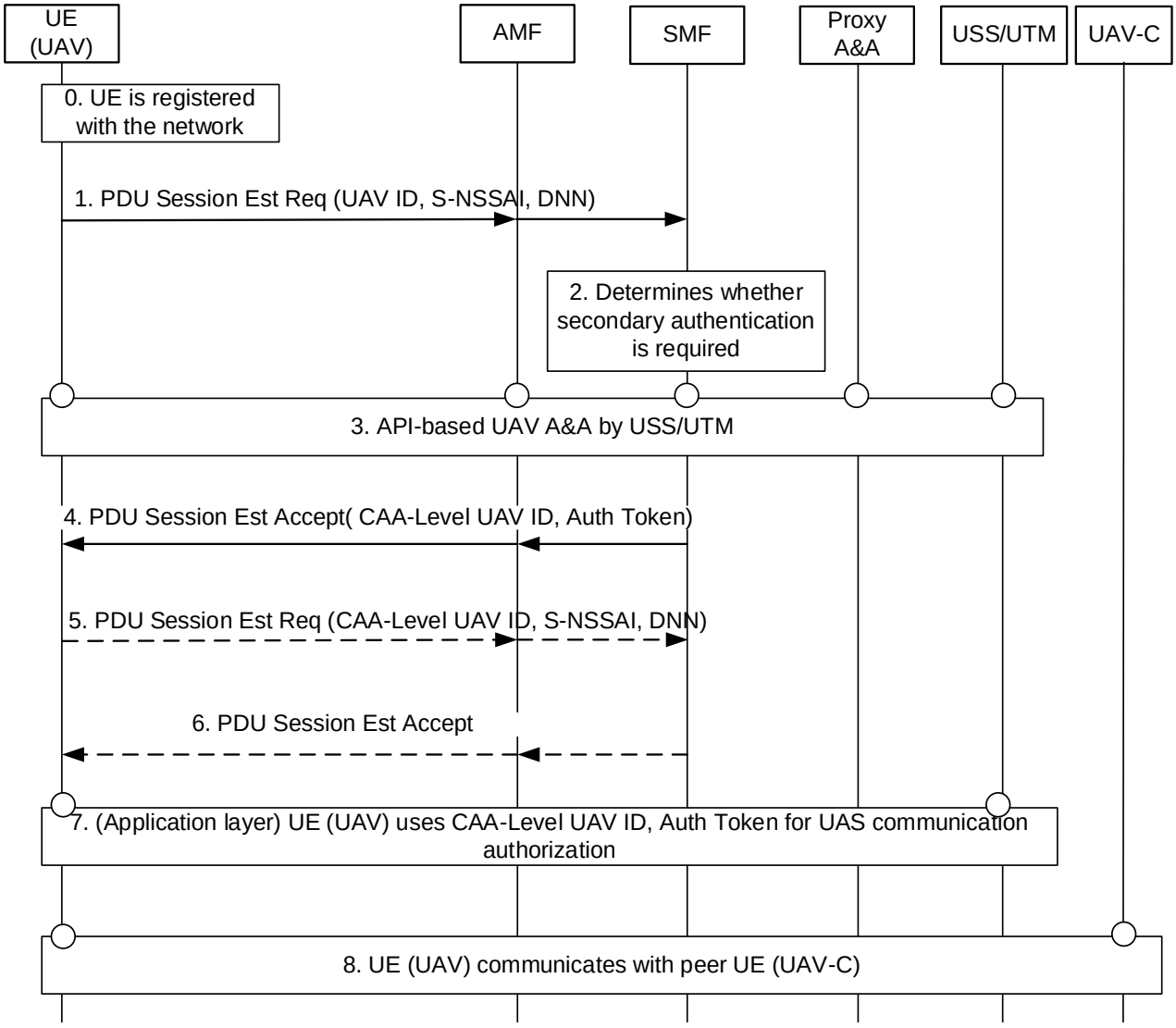


Figure 6.5.2.1-1: Procedure for UAV authentication and authorization with USS/UTM during PDU session establishment (API-based authentication)

0. The UE has successfully completed a primary authentication and is registered with the network.

1. UE sends a PDU session establishment request message that may include the following parameters: a long-term UAV ID (CAA-level UAV ID), a DNN/S-NSSAI for communicating with USS/UTM. The UE may also provide a USS/UTM address. AMF selects SMF based on UE's subscription information and DNN/S-NSSAI values. S-NSSAI/DNN may be specifically used for UAS operations with well-known values or default values configured in the UE by the network. AMF sends corresponding request to SMF.

NOTE 1: It is assumed the UE has obtained prior to this procedure the CAA-level UAV ID from a CAA and has been configured with a USS/UTM address by means outside of 3GPP scope

2. The SMF determines whether the UE is allowed for UAS operations based on subscription information and local policies.

3. The SMF triggers an API-based authentication procedure towards the USS/UTM. The SMF communicates with the USS/UTM via a Proxy A&A function (e.g., NEF) that provides an authentication API functionality. SMF or the Proxy A&A is responsible for resolving the address of the USS/UTM based on provided CAA-level UAV ID or USS/UTM address (if provided). The Proxy A&A function may authenticate USS/UTM using provisioned aviation domain certificates. The USS/UTM address may be obtained from a trusted resolution function that resolves the USS/UTM address based on the UE provided CAA Level UAV ID (if USS/UTM address was not provided by UE in step 1). During the procedure, the SMF/Proxy A&A provides the USS/UTM with a 3GPP UAV ID (e.g., GPSI as an External id) and receives from the USS/UTM a new assigned CAA-level UAV ID and authorization token and/or key material upon successful authentication and authorization. Multiple round-trips may be exchanged between the UAV and USS/UTM via SMF/Proxy A&A based on the authentication method supported by USS/UTM. During this procedure, the Proxy A&A obtains information about UAV connectivity (e.g., serving SMF ID, PDU Session ID, UAV IP address) to enable further updates of the PDU session that may be triggered by the USS/UTM (e.g., UAV authorization revocation triggered by USS/UTM as described in 6.5.2.2).

NOTE 2: How the token and/or key material is generated by the USS/UTM is outside the scope of 3GPP. The USS/UTM can for example bind the token/key material to both 3GPP UAV ID and CAA UAV level ID.

4. Upon successful authorization by USS/UTM, the SMF sends a PDU session establishment accept message that includes the new CAA-level UAV ID and authorization token and/or key material from USS/UTM.

5. The UE may additionally establish a separate PDU Session dedicated for UAS communications or modify/reuse existing PDU Session used for UAV A&A with USS/UTM. A separate PDU session is necessary if a separate DNN from the one used to communicate with USS/UTM is used for communication with a UAV-C (e.g., while the first PDU session is being used from network Remote ID functionality). The UE provides the CAA-level UAV ID obtained following the successful authorization by USS/UTM. If a UAV-C identity is known to the UAV, it may provide it during the procedure (i.e., PDU Session establishment or modification) to request pairing authorization from USS/UTM. USS/UTM notifies of pairing authorization outcome (e.g., with authorized UAV-C IP address) to the SMF (e.g., via Proxy A&A function/UAS-NF). SMF performs the configuration of the PDU Session accordingly (e.g., ACL for enforcement of pairing with UAV-C authorization).

NOTE 3: If the UAV-C identity is not known to the UAV, then it is expected that the pairing may be initiated by the peer UAV-C. The UAV may be informed of pairing authorization during a network triggered PDU Session modification triggered when USS/UTM notifies the SMF of the pairing authorization outcome and/or by application layer signalling between USS/UTM and UAV (outside of 3GPP scope).

6. The UE receives a PDU Session Establishment Accept message authorizing UAS communications. The UE may receive a new CAA-level UAV ID and optionally key material from the USS/UTM as part of a successful pairing authorization. The security parameters above (token and/or key material) when provided by the USS/UTM to the UAV are transported in transparent containers (i.e., not processed by the intermediate entities).

7. The UE establishes a secure application layer communication with the USS/UTM using the authorization token and/or key material obtained previously to further obtain UAS communication configuration from USS/UTM or perform network Remote ID reporting. The USS/UTM checks the validity of the presented authorization token.

NOTE 5: The secure application layer communication between the UAV and USS/UTM is outside of the scope of 3GPP.

8. The UE exchanges UAS traffic with peer UAV-C. The UAV and UAV-C may setup a secure connection based on key material received from USS/UTM as described in above steps.

6.5.2.2 UAV authorization revocation

The procedure for UAV authorization revocation by USS/UTM is depicted in Figure 6.5.2.2-1.

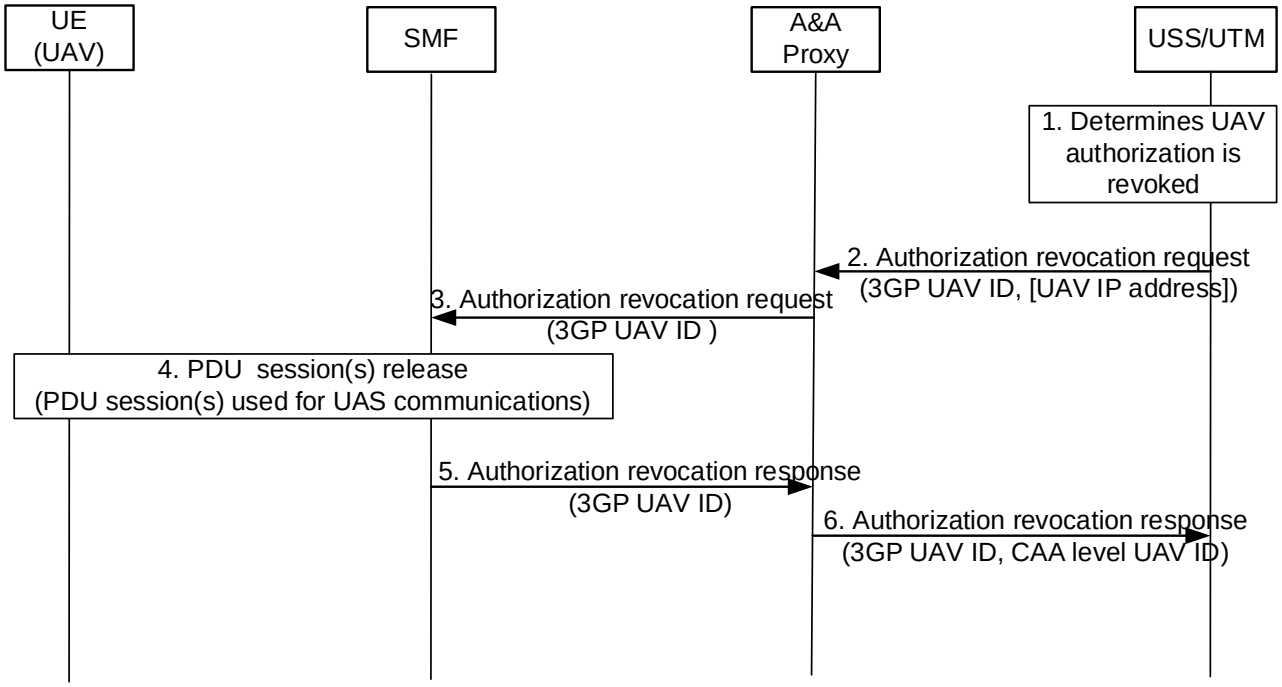


Figure 6.5.2.2-1: Procedure for USS/UTM triggered UAV authorization revocation

Pre-condition: UAV has been previously authorized by USS/UTM according to procedure 6.5.2.1.

1. The USS/UTM determines that the UAV authorization is to be revoked

2. The USS/UTM sends an Authorization revocation request to the A&A Proxy providing the 3GPP UAV ID and IP address of the PDU session allocated for the target UAV,

3. The Proxy A&A determines the SMF serving the UAV based on information maintained from procedure 6.5.2.1 and forwards the request to the SMF.

4. The SMF initiates a PDU session release procedure for the applicable PDU sessions.

7. The SMF sends an Authorization revocation response to the A&A Proxy confirming revocation of UAV authorization

8. The A&A Proxy forwards the Authorization revocation response to the USS/UTM providing the 3GPP UAV ID and CAA-level UAV ID confirming revocation of authorization for the specified UAV.

6.5.3 Solution evaluation

This solution is aligned with TR 23.754 conclusions for UUAA and pairing authorization using a PDU Session establishment/modification procedure, including the usage of a generic (API based) procedure via a UAS NF.

This solution fully addresses all requirements of Key Issue #1:

- The solution uses a generic (i.e., API based) procedure for secondary authentication of UAV by USS/UTM during PDU Session establishment (i.e., in addition to primary authentication). The UE provides its CAA-level UAV ID in the PDU Session establishment request to indicate it wants to access UAS services. The SMF triggers UUAA via a Proxy A&A (UAS NF), if the UE has a valid Aerial subscription. The authentication method and authentication messages content used during UUAA are in not in 3GPP scope.

- The solution enables the revocation of UAV authorization by the USS/UTM function via the UAS NF. The revocation may trigger a corresponding PDU Session release.

- Authentication of USS/UTM is handled by the Proxy A&A function by means of provisioned aviation domain certificates. USS/UTM address may be obtained from the UE or from a trusted resolution function which provides a USS/UTM address based on a CAA-level UAV ID.

This solution fully addresses all requirements of Key Issue #2:

- The solution enables UAV and UAV-C pairing authorization by USS/UTM. The pairing authorization is requested from USS/UTM during a PDU Session establishment/modification procedure. When pairing authorization is granted by USS/UTM, the SMF configures the PDU Session to allow C2 communication based on UAV-C peer connectivity authorization information provided by USS/UTM.

- Revocation of pairing follows similar principles as for UAV authorization revocation.

This solution fully addresses all requirements of Key Issue #6:

- The solution enables the transport of security information (e.g., token, key material) from the USS/UTM to the UE to secure communications between UAV and USS/UTM. The transport of the security information is enabled during a PDU Session establishment procedure (with UUAA). The content of the security information is not in 3GPP scope.

This solution fully addresses all requirements of Key Issue #7:

- The solution enables the transport of security information (token, key material) from the USS/UTM to the UE to secure C2 communications with UAV-C or USS/UTM. The transport of the security information is enabled during a PDU Session establishment/modification procedure (with UUAA and/or pairing authorization). The content of the security information is not in 3GPP scope.

API based procedure introduces a new mechanism compared to existing EAP framework.

NOTE 1: Usage of API based is used to address an explicit requirement from the UTM community

NOTE 2: How and whether to protect the transparent containers used for UAV-USS communication during UUAA will be determined during the normative phase

NOTE 3: IETF/3GPP protocols are readily available for EAP based mechanism to protect the transparent containers.

6.6 Solution #6: Obtaining UAV location information from the PLMN

6.6.1 Solution overview

This solution addresses Key issue #4: Location Information veracity.

6.6.2 Solution details

The solution proposes to use the currently supported location service to provide network-based location information to the USS/UTM.

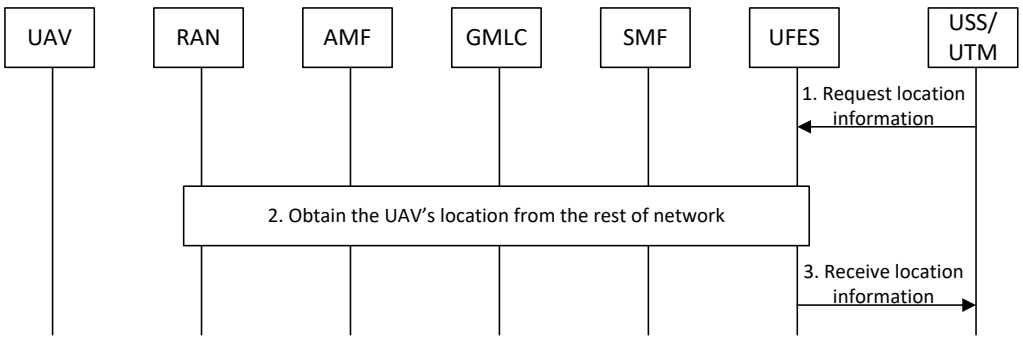


Figure 6.6.2-1: Obtaining UAV location information from the PLMN

Step 1-3 shows the procedure for the UTM/USS to obtain a network-based location for the UAV.

1. The USS/UTM sends the location request to UFES to request the UAV location from network. The USS/UTM includes the relevant identity of the UAV when the USS/UTM is requesting location information about an individual UE or a geographic area when trying to find the information of all UAVs in an area .

2. UFES uses the provided identity to obtain the identities needed to request location from the rest of the network. UFES gets the relevant UAV(s) location from AMF or GMLC by the current location services supported by AMF or GMLC.

3. UFES checks that the USS/UTM is authorised to receive the location information for a UAV.

- USS/UTM is authorised to receive the location information of a group of UAVs in a particular geographic area or of an individual UAV if it has authorised the UAV(s) for service.

- Furthermore, a USS/UTM can be authorised to receive the data about all UAV's in a particular geographic area (e.g. such an authorisation is pre-provisioned in the UFES based on regulatory requirements). The details of providing such an authorisation are left to implementation/deployments.

The UFES provides the authorised UAV(s) location information to USS/UTM for the relevant UAV. USS/UTM can use the output received at step 3 to verify the location reported by the UAV.

A similar solution is possible when the UAV is connected to EPS.

6.6.3 Solution evaluation

This solution provides a mitigation against UAV location spoofing as it ensures that network-based location information about a UAV is available to the USS/UTM.

The solution also supports the authorisation of USS/UTMs to receive only the UAV location information about either UAVs under the USS/UTM control or if all the UAVs in a geographic if specifically authorised to receive this information.

6.7 Solution #7: UAS authentication, authorization and security aspects

6.7.1 Solution overview

The solution address key issue #1 and #6.

This solution assumes the following based on TR 23.754 Clause 4.2 Architecture assumptions.

- A UAV is assigned, a CAA-level UAV Identity by functions in the aviation domain (e.g. USS) or by functions in the USS/UTM.

- The 3GPP CN is aware of the CAA-level UAV Identity. A mapping shall be possible in the mobile operator network and in the UAS application layer outside of 3GPP between the 3GPP UAV ID and the CAA-level UAV ID.

The solution also further assumes that, the long-term security credentials for UAV were also assigned and provided along with the CAA-level UAV ID by the USS/UTM which is out of 3GPP scope.

This solution is applicable to EPC and 5GS.The solution addresses the following:

- Enables USS/UTM to authenticate and authorize the UAV(s) to access and use the USS/UTM services securely.

NOTE 1: The same mechanism can be applied to a networked UAV Controller when required.

6.7.2 Solution details

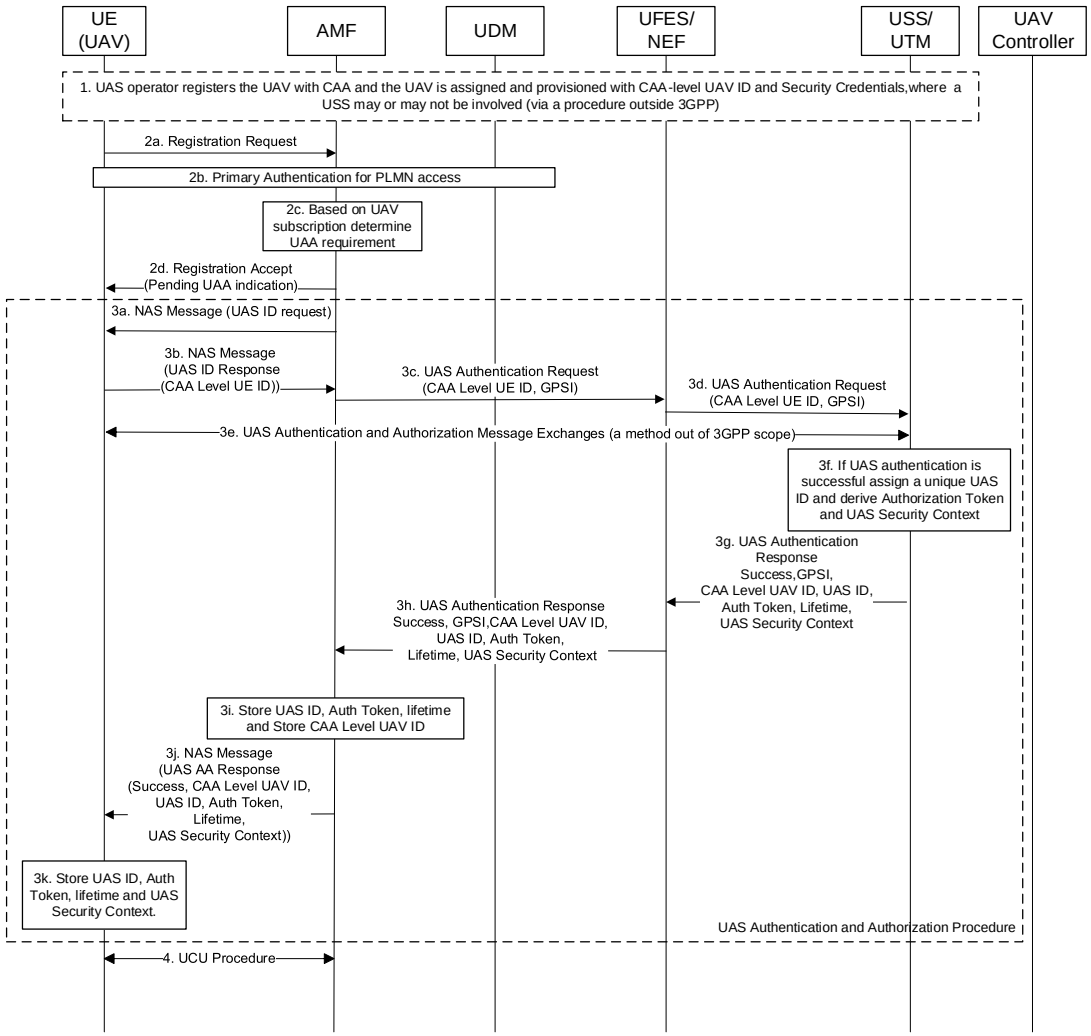


Figure 6.7.2-1: UAS authentication and authorization (UAA) procedure

Step 1. As a precondition the UAV is registered with the USS/UTM by the UAS operator using any method outside the 3GPP scope. During this registration, the UAV is configured with the CAA-level UAV ID, the USS routing information (which may also be part of CAA-level UAV ID), and the required long-term credentials to enable UAS security. These are the credentials that are provisioned into the UAV to form the root of the UAS security. The credentials may include symmetric key(s) or public/private key pair (example. with certificates) depending on the implementation which is out of 3GPP scope.

Step 2a-b. The UAV sends registration request to AMF and a primary authentication is performed as specified in TS 33.501.

Step 2c. After a successful primary authentication, the AMF based on the UE (UAV) subscription information fetched from the UDM/UDR determines to trigger UAS authentication and authorization (UAA).

NOTE 1: The UAA can also be performed when an UAV requests a PDU session establishment for any UAS service (i.e., USS/UTM) by including the CAA-Level UAV ID in the PDU Session establishment Request message where the UAA related message exchange is performed involving the SMF.

Step 2d. AMF sends to UE (UAV) an UAS authentication Required Indicator or a pending UAA indication in the Registration Accept message.

Step 3a. AMF may optionally send an UAS ID request to the UAV over the NAS transport.

Step 3b. The UAV responds to AMF with a UAS ID response containing CAA-level UAV ID and optionally USS routing information (if routing information is not part of CAA-level UAV ID).

Step 3c. Based on the USS routing Information, the AMF sends a UAS Authentication request message (i.e., over a service-based interface) to the UFES. The GPSI can be used for external identification of UAV. The routing to a UFES and USS/UTM and external ID usage need to be aligned with SA2 agreements during the normative work.

NOTE 2: The new 3GPP UAS Network Function specified in SA2 TR 23.754 conclusion is referred as UFES in this solution. The actual naming for the new 3GPP UAS Network Function which handles the UAS related operational message exchange between 5GS/EPS and USS/UTM can be defined during the normative phase.

Step 3d. The UFES forwards the received UAS authentication request message to the appropriate USS/UTM.

Step 3e. The USS/UTM performs authentication method specific message exchange with the UAV to enable mutual authentication. The authentication method used for UAA is up to USS/UTM and it is out of 3GPP scope.

Step 3f. The USS/UTM on performing a successful UAS authentication, verifies the preconfigured CAA Level UAV ID based on the stored UAV subscription, if required assign a new CAA Level UAV ID to the UAV. Further the USS/UTM assigns a UAS ID to uniquely identify the UAS formed by the UAV and associated UAV-C information based on UAS subscription. The method of UAS-ID assignment is out of 3GPP scope. Further the USS/UTM shall generate a UAS root security context (based on a method out of 3GPP scope) from the long-term credential available as part of UAS subscription information in the USS/UTM to enable UAS security and a n UAS root security identifier (e.g., bound to the security context)shall be generated to uniquely identify the UAS root security context in the USS/UTM. To enable authorization of UAV for various UAS service following a UAS registration (example., flight authorization request, PDU session establishment for C2 and Pairing of UAV with UAV-C etc.,), the USS/UTM shall generate an Authorization Token (Auth Token) (e.g., it can be bound to the UAS ID, UAV-CAA-Level ID, optional UAV-C ID). The USS/UTM also assigns a lifetime (a validity period or time duration) for the authorization token for it to be used by the 3GPP network to authorize the UAV for various subsequent UAS services. The USS/UTM after successful UAS authentication, locally stores the External ID of UAV (i.e., GPSI), CAA-level UAV ID, authentication status information, UAS ID, Auth Token, lifetime along with UAS Security Context and its identifier. The UAS root security context (e.g., a key) and its corresponding identifier forms the UAS security context. Optionally, if the UAV has no preconfigured UAV-C ID, the USS/UTM may also provide the UAV-C ID for the UAV along with the UAV authentication response.

Step 3g. In response to the successful UAS authentication, the USS/UTM sends the UAS authentication response message to the UFES. The UAS authentication response message includes an authentication result with Success Indication, GPSI, CAA Level UAV ID, UAS ID, UAS security context, Auth Token and lifetime.

Step 3h. The UFES receives the UAS authentication response message containing Success Indication, GPSI, CAA Level UAV ID, UAS ID, UAS security context, Auth Token and lifetime as part of the UAS information for the UAV. The UFES stores the received UAS information for the UAV and the parameters exactly stored at UFES will be defined during the normative phase. Further, the UFES forwards the received UAS authentication response message to the AMF.

Step 3i. The AMF receives the UAS authentication response message and locally stores the received authentication result with Success Indication, CAA Level UAV ID, UAS ID, Auth Token and lifetime as part of the UAS information for the UAV to enable subsequent UAS service authorization at the 3GPP network.

Step 3j. The AMF forwards the received UAS authentication response message to the UAV.

Step 3k. The UAV receives the UAV authentication response message and on receiving a ‘Success Indication’, the UAV generates the UAS Security context (UAS root security context and identifier) similar to the USS/UTM from the long-term credential preconfigured in the UAV. If the locally generated UAS security context and received UAS security context matches, then the UAV considers the UAS authentication as successful and locally stores the received CAA Level UAV ID, UAS ID, Auth Token, lifetime, UAS root security context and its identifier along with the most recently derived K_{UAS} as part of UAS Security Context. The UAV uses the UAS root security context identifier to uniquely identify the UAS root security context. The UAS root security context can be used by the UAV and USS/UTM to set up secure connection.

Step 4. The AMF may trigger UE parameter update procedure as specified in TR 23.754.

UAS Authentication and Authorization (UAA) Revocation:

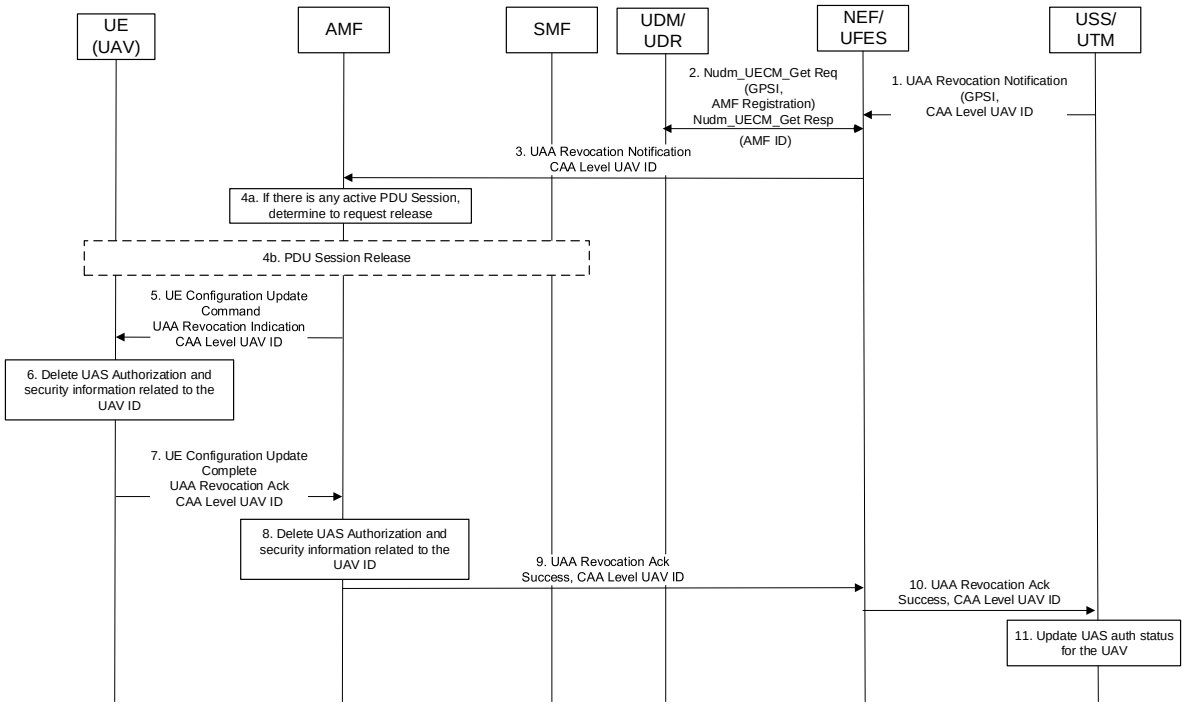


Figure 6.7.2-2: UAS authentication and authorization (UAA) Revocation procedure

Step 1. The USS/UTM determines to revoke UAS authentication and authorization corresponding to an UAV identified with CAA Level UAV-ID and sends an UAA Revocation Notification with GPSI and CAA Level UAV ID to the corresponding UFES using a service operation message.

Step 2. The UFES fetches the serving AMF ID corresponding to the GPSI of the UAV from the UDM by invoking Nudm_UECM_Get Request/Response message based on TS 23.502 Clause 5.2.3.2.4.

Step 3. The UFES sends the received UAA Revocation Notification message to the AMF with the CAA level UAV ID.

Step 4a-b. The AMF on receiving the UAA Revocation Notification, if there is any related active PDU session corresponding to the UAV, initiates a PDU Session release based on TS 23.502 Clause 4.3.4.

Step 5. The AMF further enables the UAA revocation with the UE using the UE Configuration update procedure. The AMF sends CAA Level UAV ID along with the UAA Revocation indication to the UAV in the UE Configuration update command.

Step 6. The UAV on receiving the UAA Revocation indication, shall delete all the UAS authorization and security information locally stored corresponding to its CAA Level UAV ID.

Step 7. The UAV further sends to AMF, a UE Configuration update complete message with a UAA Revocation acknowledgement along with the CAA Level UAV ID.

Step 8. The AMF on receiving the UAA Revocation acknowledgement and CAA Level UAV ID, deletes locally stored UAS authorization and security information corresponding to the UAV ID.

Step 9a. The AMF further sends an UAA Revocation acknowledgement message with Success Indication, GPSI and CAA Level UAV ID to the UFES.

Step 9b. The UFES removes UAV related information (if any) locally stored related to the UAV.

Step 10. The UFES further sends the received UAA Revocation acknowledgement message with the received Success Indication, GPSI and CAA Level UAV ID to the USS/UTM.

Step 11. The USS/UTM on receiving the UAA Revocation acknowledgement message with Success Indication, GPSI and CAA Level UAV ID, updates the UAS authentication status and related information locally stored for the UAV.

Applicability to EPS:

The UAS Authentication and Authorization procedure and revocation procedure described in this section can be applicable to EPS, with the adaptation of MME, SMF+PGW-C, UPF+PGW-U and HSS+UDM respectively as described in the steps below. UFES can act as a UAS NF or UAS control function in the 3GPP network which can be a standalone network function, or a service offered by the SCEF in the EPS instead of NEF in the 5GS. For the UAA revocation procedure, the MME, S-GW+PGW-C and HSS will be involved in EPS. The message name used in EPS procedure can be aligned with SA2 where required during the normative work. The steps related to UAA for an UAV in EPS scenario is described as follows:

Step 1. The precondition is applicable as described for 5GS case.

Step 2. The UAV sends Attach request to MME and an authentication and key agreement is performed. The UAV can send a CAA level UAV ID with USS Routing information, Flight path data and target UAV-C information if any during the attach request or after authentication in a NAS message.

Step 3. The MME, based on the subscription information, selects the Default APN for connectivity with the USS/UTM based on 23.754. The MME can send to SMF+PGW-C via SGW, a create session request which contains the CAA level UAV ID and flight path data and target UAV-C information if any and 3GPP UAV ID (i.e., an external identifier). The MME receives a create session response form SMG+PGW-C and an attach accept is provided to the UAV.

Step 4. The SMF+PGW-C sends a UAV authentication request to the UFES (or a UAS NF as mentioned in 23.754) with CAA level UAV ID and flight path data and target UAV-C information if any and 3GPP UAV ID.

Step 5. The UFES forwards the received UAS authentication request message to the appropriate USS/UTM.

Step 6. The USS/UTM performs authentication method specific message exchange with the UAV to enable mutual authentication. The authentication method used for UAA is upto USS/UTM and it is out of 3GPP scope. Then Step 3f and 3g (Figure 6.7.2-1) is similar as described for 5GS.

Step 7. In response to the successful UAS authentication, the USS/UTM sends the UAS authentication response message to the UFES. The UAS authentication response message includes an authentication result with Success Indication, 3GPP UAV ID, CAA Level UAV ID, UAS ID, UAS security context, Auth Token and lifetime.

Step 8. The UFES receives the UAS authentication response message and may store any received UAS information for the UAV. Further, the UFES forwards the received UAS authentication response message to the SMF+PGW-C.

Step 9. The SMF+PGW-C sends update bearer request with the information received in UAS authentication response message to the MME.

Step 10. The MME forwards the received UAS authentication response message to the UAV in a NAS message. The UAV receives the UAV authentication response message and then the process in UAV is same as described in step 3k (Figure 6.7.2-1) for 5GS and sends a response to MME.

Step 11. The MME further confirms to SMF+PGW-C with update bearer response. The MME/SMF+PGW-C locally stores the received authentication result with Success Indication, CAA Level UAV ID, UAS ID, Auth Token and lifetime as part of the UAS information for the UAV to enable subsequent UAS service authorization at the 3GPP network. The SMF+PGW-C can set the traffic filters to allow traffic between UAV and USS/UTM based on the authentication result

The UAA revocation in EPS for any UAV can be performed as follows:

Step 1. The USS/UTM determines to revoke UAS authentication and authorization corresponding to an UAV identified with CAA Level UAV-ID and sends an UAA Revocation Notification with 3GPP UAV ID (i.e., external identifier) and CAA Level UAV ID to the corresponding UFES.

Step 2. The UFES sends the received UAA Revocation Notification message to the SMF+PGW-C (the serving PGW can be identified based on 23.754).

Step 3. The SMF+PGW-C on receiving the UAA Revocation Notification, initiates a PDN connection release and during the PDN connection release procedure, it provides to UAV via the SGW and MME, the CAA level UAV ID and UAA Revocation indication based on the received UAA Revocation Notification message.

Step 4. The UAV on receiving the UAA Revocation indication, can delete all the UAS authorization and security information locally stored corresponding to its CAA Level UAV ID.

Step 5. The UAV further responds to MME, with a UAA Revocation acknowledgement along with the CAA Level UAV ID.

Step 6. The MME sends the received UAA Revocation acknowledgement and CAA Level UAV ID, to SMF+PGW-C, which can delete the locally stored UAV information.

Step 7. The SMF+PGW-C send the UAA Revocation acknowledgement along with the CAA Level UAV ID to the UFES.

Step 8. The UFES removes UAV related information (if any) locally stored related to the UAV. The UFES further sends the received UAA Revocation acknowledgement message with the received Success Indication, GPSI and CAA Level UAV ID to the USS/UTM.

Step 9. The USS/UTM on receiving the UAA Revocation acknowledgement message with Success Indication, GPSI and CAA Level UAV ID, updates the UAS authentication status and related information locally stored for the UAV.

6.7.3 Solution evaluation

The solution allows USS/UTM (post successful UAA) to send the UAS security context (a security information and identifier), UAS ID, Auth Token and lifetime to the UAV. Following a successful UAA, the solution requires generation of authorization information (i.e., Auth Token) by USS/UTM to allow authorization information to be provided to the UAV to enable further UAS service authorization. The UAS security context can be used to set up secure connection between UAV and USS/UTM. As 23.754 allows sending new CAA level UAV ID to UAV, a dedicated identifier is most crucial to be provided by the USS/UTM to identify the security context provided to the UAV. The Auth Token can be used to enable authorization of UAV for subsequent UAS service. The UAS ID can allow identification of an UAS formed by the UAV, USS/UTM and UAV-C as applicable (UAS ID generation is upto USS/UTM and it is outside the scope of 3GPP).

AMF in 5GS and SMF+PGW-C in EPS: On a successful UAA, store information such as authentication result (i.e., success) along with information received in UAS authentication response (i.e., CAA level UAV ID, UAS ID, Auth Token and lifetime. Optionally UAVC ID if received), which can enable subsequent UAS service authorization.

On a UAA Revocation Notified by USS/UTM, release PDU session/PDN Connection by indicating UAA Revocation Indication and CAA Level UAV ID to UAV. Delete any UAV related information locally stored related to CAA level UAV ID.

UE: On a successful UAA, store information such as authentication result (i.e., success) along with information received in UAS authentication response (i.e., CAA level UAV ID, UAS Security Context, UAS ID, Auth Token and lifetime. Optionally UAVC ID if received), which can enable subsequent UAS service authorization and security set up.

On receiving UAA Revocation Indication and CAA Level UAV ID, delete all information related to UAA such as UAS Security Context, UAS ID, Auth Token, lifetime, and any CAA level UAV ID (if meant for temporary use).

Credentials used by UAV and UTM/USS are out of 3GPP scope.

6.8 Solution #8: Using 5G location result for location information verification

6.8.1 Solution overview

This solution addresses Key Issue 4 to support the location Information veracity. USS/UTM requests the location service to 5GS with a requirement of high reliability. If the network-assisted positioning method as defined in clause 6.11.2 in TS 23.273[5] is chosen, the location result will not depend on the UE's report. The location result from 5GS can be utilized to verify the location information which is reported from UE side.

6.8.2 Solution details

5GS already provides the location service (LCS). Location information for one or multiple target UEs may be requested by and reported to an LCS client or an AF within or external to a PLMN. The procedure of the location information veracity can be described as follows:

1. USS/UTM receives the location information which is reported by UE via the application layer. If UTM/USS decides to check and verify the location information, UTM/USS sends a request to the GMLC for a location and optionally a velocity for the target UE which may be identified by a GPSI. The LCS request also carries the requirement of high reliability, which indicates the 5GS to select the positioning method which is not based on the UE's report.

2. GMLC continues with the location service procedure as defined in clause 6.1.2 in TS 23.273 [5] and indicates LMF to select Network Assisted Positioning method. Network Assisted Positioning method relies on the location measurement from NG-RAN nodes.

3. The LMF invokes the Namf_Communication_N1N2MessageTransfer service operation towards the AMF to request the transfer of a Network Positioning message to a NG-RAN node (gNB or ng-eNB) in the NG-RAN. The target NG-RAN node obtains and returns the position related information.

4. The LMF calculates the location result and responds to GMLC.

5. USS/UTM aquires the location information from GMLC and verifies the information from the application layer. USS/UTM may make decisions to control the UAV/UAVC based on the verification result.

NOTE: If USS/UTM is regarded as AF, it does not directly interact with GMLC and the interaction may be done via NEF or UFES.

6.8.3 Solution evaluation

This solution fulfills the requirement in Key Issue 4.

The solution reuses the existing location service provided by 5GS. The Network Assisted Positioning method can be regarded as trusted as it does not rely on the UE's report. Based on the result of the verification, USS/UTM may make decisions to control the corresponding UAV/UAVC.

6.9 Solution #9: UAS enabled authentication

6.9.1 Introduction

This solution addresses the key issue #1 UAS Authentication and Authorization.

When a UAV type UE registers to 5GS, it will after a first successful authentication also register with USS/UTM. The solution proposes to optimize for UAS authentication.

6.9.2 Solution details

When a UAV type UE sends a registration request, it includes in SUCI an indication "UAV type" (step 1) to indicate to the 5GS that additional authentication is needed. After successful authentication, the AUSF provides in its authentication response this UAV type information to AMF (step 2). By this, the AMF knows that the UE is a UAV type UE that also wants to connect to USS/UTM system. I.e. this is to indicate to the serving network the service, for which the UAV enabled UE wants to be authenticated and AMF requests the UAV ID from the UE (step 3).

The 3GPP system is aware of the 'CAA-level UAV ID' and its mapping with 3GPP UAV ID. If the UAV-type UE (UAV/UAV-C) has successfully authenticated to 5GS, it shares within the SMC response its 'CAA level UAV ID' with AMF (step 4).

NOTE: SMC message is extended to support UAS IDs.

AMF retrieves 3GPP UAV ID from UDM database (step 5). A mapping of SUPI, CAA level UAV ID and 3GPP UAV ID is performed in UDM (step 6) and 3GPP UAV ID is provided back to AMF (step 7). Now UAV/UAV-C authentication and authorization towards UTM/USS can be triggered by AMF (step 8).

Editor's note: Whether the storage of CAA-level UAV Id in UDM is needed in addition to CAA-level UAV Id storage in UAS NF is FFS

Editor's note: Which intermediate functions are involved between AMF and USS/UTM is ffs.

Editor's note: Whether a communication between UAV and UTM is needed in steps 8 and 9 is ffs.

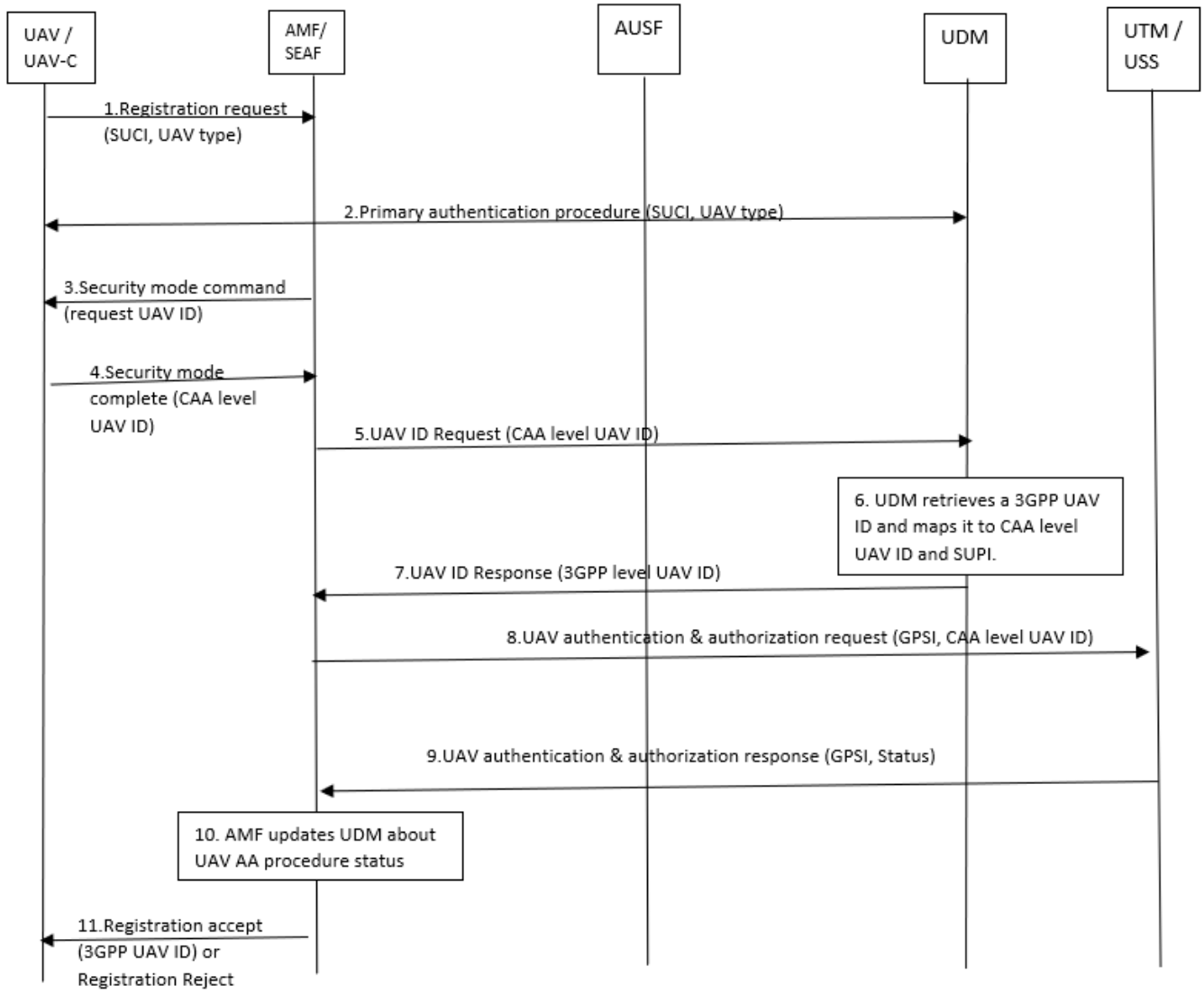


Figure 1

Figure 6.9.2-1: UAS enabled authentication flow

After successful authentication and authorization by UTM/USS, UAV authentication and authorization response is sent to AMF with external identifier (step 9). In case of failure, UAV Authentication & Authorization response is sent to AMF with a failure status. AMF updates UAV authentication and authorization results to UDM (step 10). Also, the UAV/UAV-C is informed with registration accept or reject message (step 11).

If the UDM did not have an entry for the 'CAA-level UAV ID', i.e. it is a non-registered UAV-type UE, then depending on operator policy the UAV/UAV-C may be registered in UDM, the UE becomes a subscriber for a service and a 3GPP UAV ID is provided.

6.9.3 Evaluation

TBD

6.10 Solution #10: Authentication and authorisation of UAVs

6.10.1 Solution overview

This solution addresses Key issue #1: UAS Authentication and Authorization.

6.10.2 Solution details

6.10.2.1 General

The solution uses a UAV Flight Enablement Subsystem (UFES) as a single point of contact between the PLMN and USS/UTM in order to limit the impact on the 3GPP system, although it is not strictly necessary for authentication and authorisation solution to work. The authentication and authorisation procedures are shown when connected in 5G and the authentication/authorisation takes place after registration, but similar procedures could be used during registration and also during PDU connection establishment with the SMF playing the role of the AMF. The procedure in 6.X.2.2 are used to authenticate and authorized UAV so connectivity for UAS services can be enabled

6.10.2.2 Authentication and authorisation of a UAV

Figure 6.10.2.2-1 shows how the UAV can be authenticated and authorised by the USS/UTM to access the 3GPP network as a UAV, i.e. it is assumed in these flow that the authentication and authorisation will happen.

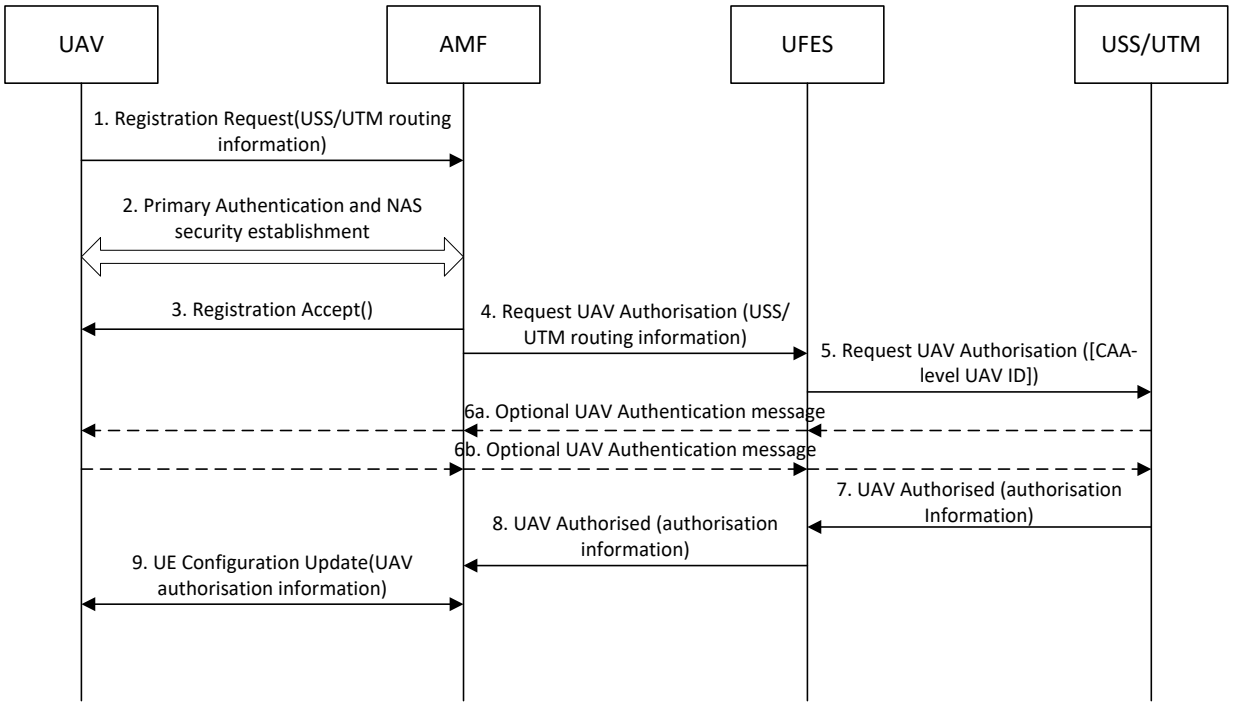


Figure 6.10.2.2-1: Authentication and authorisation of a UAV

The steps are as follows:

1. The UAV sends a Registration Request to the AMF requesting to register as UAV. The UE includes USS/UTM routing information in the Registration Request message.

NOTE 1: How the UE signals it is requesting to register as a UAV is left to stage 3 specification.

NOTE 2: The details of the how the USS/UTM is selected from USS/UTM routing information is left to the stage 3 specification. One possibility is a CAA-level UAV ID. If this is not supplied this ID can be requested during steps 6a and step 6b when authenticating and authorising the UAV.

2. Primary authentication and NAS security establishment are performed.

3. The AMF sends the Registration Accept message to the UAV indicating that the UAV needs to be authorised by the USS/UTM.

NOTE 3: At this point the UAV has restricted access to PDU sessions.

4. Based on subscription information and local policies, the AMF requests UAV authentication and authorisation from UFES including the USS/UTM routing information. The UFES is selected using the USS/UTM routing information.

5. The UFES triggers an authentication and authorisation request including the CAA-level UAV ID if available from the USS/UTM. The correct USS/UTM is selected using the USS/UTM routing information and a USS/UTM will only be selected if it has been authorised to act as one. The UFES includes the 3GPP UAV ID in the request

NOTE 4: Whether the 3GPP UAV ID is sent from the AMF or retrieved (from other network entities) using the SUPI is left to stage 3 specification.

6a. and 6b. There can be several round trips required for authentication of the UAV by the UTMs depending on the authentication method used by the USS/UTM and UAV. The authentication method and the content of messages used for authentication are out of scope of 3GPP. The content of the messages is carried in containers that are passed along and not processed by the entities between the UAV and USS/UTM.

7. On a successful authentication and authorisation of the UAV, the USS/UTM stores the 3GPP UAV ID with the CAA-level UAV ID. The UTMS/USS informs the UFES that the UAV has been successfully authenticated and authorised by the USS/UTM. The USS/UTM includes authorisation information for both the network and the UAV.

8. The UFES further informs the AMF that the UAV has been successfully authenticated and authorised by the USS/UTM. The UFES passes the received authorisation information onto the AMF.

9. The AMF stores the network authorisation information as part of the UE context. The network authorisation information further contains the information whether USS/UTM authentication and authorisation is required during future registrations and whether to allow UE to establish PDU session(s) dedicated for the UAS service with or without further USS/UTM authentication and authorisation.

NOTE 5: The lifetime of the authorisation, e.g. permanent till revocation or one time authorization, is left to the normative phase.

The AMF triggers a UE Configuration Update (UCU) procedure to inform the UE that the UAV authentication and authorisation has been successful. The UCU procedure contains the UAV authorisation information. Part of the contents of the UAV authorisation information may be passed to the UAV without modification by any entities between USS/UTM and UAV. The UAV uses the UAV authorisation information to check if it is authorised by the network to act as a UAV and also to receive any needed aviation information if any, e.g. a CAA-level UAV ID.

NOTE 6: Before step 9, the UE has restricted access to PDU sessions. After step 9, there are no restrictions, although a further authentication and authorisation might be required during PDU session establishment.

6.10.2.3 Revocation

Figure 6.10.2.3-1 show how the authorisation can be revoked.

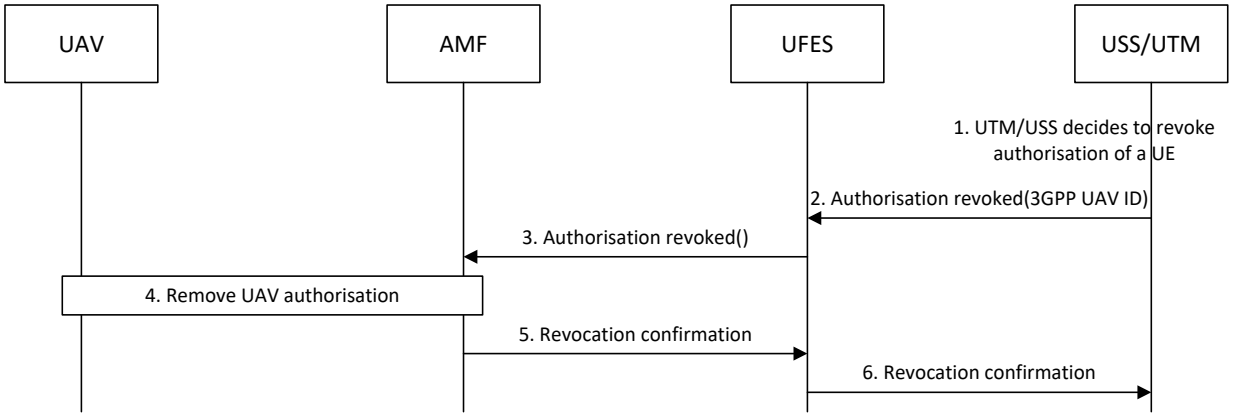


Figure 6.10.2.3-1: UAV revocation

The steps are as follows:

1. The USS/UTM decide to revoke the UAV's authorisation.

2. The USS/UTM sends an Authorisation Revoke request to the UFES including the 3GPP UAV ID of the UAV to be revoked.

3. The UFES passes the Authorisation Revoke request to the AMF.

4. The AMF revokes the authorisation to act like an UAV. A consequence of the revocation is to release of all connections.

NOTE 1: Messages used to perform revocation are left to stage 3. Whether all connections or only connections dedicated to the UAS service are released is left for the normative phase.

5. The AMF confirms to the UFES that the revocation has happened.

6. The UFES confirms to the USS/UTM that the revocation has happened.

6.10.3 Solution evaluation

This solution addresses key issue #1 during registration to a 5G network. The solution provides a method for the USS/UTM to authenticate and authorise a UAV before the UAV can access UAS services from the 3GPP system. The solution also provides a method of revoking the authorisation and only authorised USS/UTMs can provide the authorisations for UAVs.

6.11 Solution #11: UAV and UAVC pairing authorization through bound IDs

6.11.1 Solution overview

This solution addresses the key issue #2: Pairing authorization for UAV and UAVC.

This solution assumes UAV and UAVC are equipped with SUPI and credentials from PLMN. The pairing authorization is performed after UAV or UAVC is authenticated by 3GPP systems through Primary authentication. It is performed when UAV is being authenticated/authorized, or after it has been authenticated/authorized by USS/UTM.

6.11.2 Solution details

6.11.2.1 UAV and UAVC pairing authorization

A general overview of the procedure involving UAV and UAVC paring authorization is shown in Figure below.

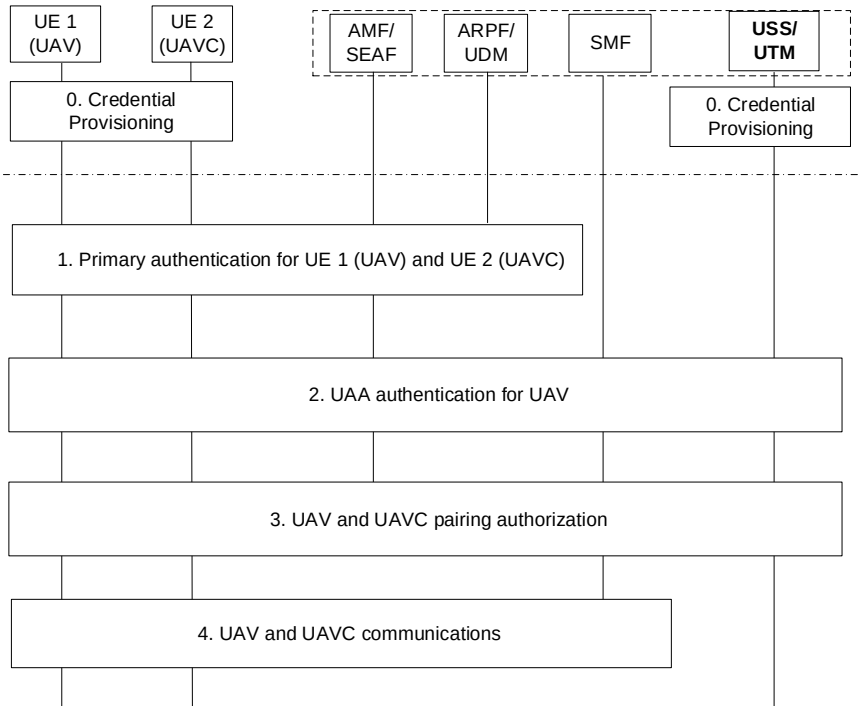


Figure 6.11.2.1-1: A general overview on UAV and UAVC pairing authorization

0. Provisioning:

a. UAV and UAVC: provisioned with UAV IDs and corresponding credentials, e.g. their private/public key pairs and certificates issued by UAS service providers/operators. Regarding pairing, there are two options considered: 1) provision is not required, it will be provisioned at USS/UTM 2) pairing is provisioned at both UAV and UAVC, e.g. indicated using certificates.

b. USS/UTM: provisioned with its private/public key pairs. The UAS service providers/operators have registered their public keys or their root CAs with USS/UTM so that USS/UTM can verify their issued certificates. Regarding pairing, similarly, there are two options: 1) pairing of UAV and UAVC has been provisioned and UAV-ID and UAVC-ID are bound together; 2) no pairing information provisioned.

NOTE 1: UAV and UAVC pairing shall not be determined by other parties than USS/UTM or UAS itself, e.g. between UAV and UAVC. The provisioning is out of scope of 3GPP.

1. Primary Authentication: UE1 (UAV) and UE2 (UAVC) are equipped with SUPI and 3GPP credentials and need to perform Primary Authentication as normal UEs before getting UAS services.

2. For UAS-type UE, UAS authentication is performed for UAV.

NOTE 2: UAV authentication is not addressed in this solution. This steps is to indicate pairing is for authenticated and authorized UAV.

3. USS/UTM authorize UAV and UAVC pairing

a. Case 1 (pairing information is provisioned at USS/UTM): based on bound UAV-ID and UAVC-ID to determine whether pairing request from UAV (with UAV-ID and GPSI) or UAVC (with UAVC-ID and GPSI) can be authorized.

b. Case 2 (UAV-ID and UAVC-ID are paired and bound): based on bound information sent from UAV or UAVC to determine whether pairing request from UAV (with UAV-ID and GPSI) or UAVC (with UAVC-ID and GPSI) can be authorized. USS/UTM may need to verify the certificates presented by UAV/UAVC.

NOTE 3: UAV (or UAVC) does not send GPSI to AMF. Instead, it sends UE ID (e.g. GUTI or SUCI) as a normal UE and AMF will convert the UE ID into GPSI.

3-1. UAV sends a pairing request message, e.g. in a PDU Establishment Request message to USS through the network (e.g. AMF or SMF and UFES). The message will include UAV-ID and its UE ID (e.g. GUTI). For Case 2, it includes UAV-ID (and UE ID if available) of the paired UAVC as well.

3-2. USS determines whether to authorize the pairing of UAV and UAVC

3-3. USS informs PLMN and UAV the authorization results. The message includes UAV-ID and GPSI of the UAV. and It may include the UAVC-ID and GPSI of the paired UAVC if available. Based on the results, the PLMN (e.g. SMF) may determine whether the PDU session is authorized for UAV and UAVC communications.

NOTE 4: step 3 and step 2 may be combined depending on scenarios.

4. UAVC communicates with UAV through UPF (UP).

6.11.2.2 Revocation

USS/UTM may trigger revocation pairing of UAV and UAVC pairing at any time. The call flow is shown in the figure 6.11.2.2-1.

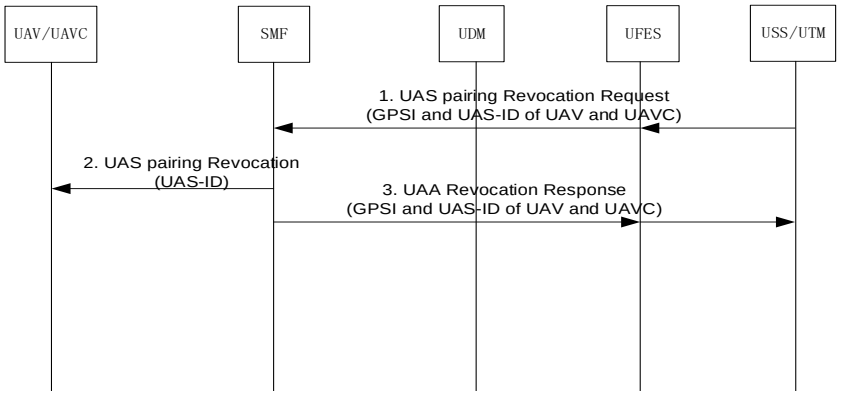


Figure 6.1.2.2-1: UAS pairing revocation procedure

1. The USS/UTM sends the UAA revocation request to SMF through UFES to revoke the UAVC pairing for a UAV. The UAV and UAVC are dentified by their GPSI and UAS-ID respectively in the UAA revocation Request.

NOTE: UFES is an NF interfacing USS/UTM and it can locate SMF serving the UAV.

2. The SMF may inform UAV or UAVC with the UAA pairing revocation message.

3. The SMF responses USS that the pairing of UAV and UAVC has been revocated.

6.11.3 Solution evaluation

This solution addresses the key issue #2.

In this solution, pairing information is assumed to be pre-provisioned, 1) provisioned at USS/UTM; 2) provisioned at UAV/UAVC (the provisioning is not scope of 3GPP). Pairing authroization is performed at USS/UTM after UAV is authenticated by PLMN. Pairing authorization is sent to PLMN with associated IDs (e.g. GPSI and/or UAV IDs).

This solution supports pairing revocation triggered by USS/UTM at any time. Editor's note: Further evaluation is ffs on SMF enforcing authorization of C2 traffic.

6.12 Solution #12: UAV location privacy protection

6.12.1 Solution overview

The contribution proposes a solution to address the following key issues:

- KI#5 " Privacy protection of UAS identities ".

- The fake USS/UTM issue part of KI#1 is also addressed in this solution.

- KI#4 for the location tracking authorization.

Solution #25 in TR 23.754 [3], adopted as the basis for normative work for UAV location tracking, includes the support for a new "unknown UAV tracking" feature. This feature allows a given USS/UTM to obtain a list of UAVs that are present in a specified target area. Currently, solution#25 does not have any provision to prevent exposure of UAV location information to unauthorized USS/UTM (e.g., competitor USS/UTM).

This solution proposes enhancements to solution #25 to ensure that only authorized entities (e.g., USS/UTM serving the UAV) can obtain location information for a UAV or set of UAVs from the 3GPP system.

The solution assumes (as per TR 23.754 [3] clause 8.5) that UAV location information is provided to USS/UTM via a UAVF which may encompass the NEF/SCEF functionality.

6.12.2 Solution details

6.12.2.1 USS/UTM identifier association with individual UAV during UAV A&A

During a UAV A&A procedure, UAVF and/or AMF stores a USS/UTM identifier (e.g., FQDN or IP address of the USS/UTM) and associates it with the 3GPP UAV ID (e.g., GPSI) and the CAA level UAV ID of the UAV that is successfully authenticated and authorized. The USS/UTM identifier may be obtained from the UE during the UAV A&A procedure (e.g., in Registration or PDU Session establishment request). The UAVF authenticate the USS/UTM using aviation domain provisioned certificates. If the UE did not provide a USS/UTM address, the UAVF may also resolve the USS/UTM address based on the UE provided CAA Level UAV ID by means of a trusted resolution function (UAVF may play the role of such resolution function when 3GPP assisted CAA-level UAV ID allocation is used).

During UAV location tracking procedure, the UAVF which verifies that the location tracking request is authorized (i.e., checks that identifier of the USS/UTM making the request matches the USS/UTM identifier previously associated with the 3GPP UAV ID during UAV A&A procedure).

NOTE: It is assumed that the location request from USS/UTM can be authenticated by UAVF (e.g., using aviation domain provisioned certificates).

6.12.2.2 Verification of USS/UTM authorization for unknown UAV location tracking

When receiving an "unknown UAV" location tracking request from a USS/UTM, The UAVF checks the validity of the request (described in 6.X.2.1) before forwarding the request to the appropriate location tracking function (e.g., AMF, GMLC). The request includes an indication that the request is for any (e.g., unknown) UAV(s) in the target area.

The AMF obtains location information of all the UAVs in the given area. The AMF may perform filtering of UEs in that area such as to select only those that fullfill relevant UAV selection criteria (e.g., with a valid UAV subscription and/or that have been authorized by a USS/UTM, as per TR 23.754 [3] clause 8.5). The AMF sends the location information to the UAVF for each of the UAVs that are in the given area including the 3GPP UAV ID for each UAV.

For each UAV, the UAVF selects UAVs whose 3GPP UAV ID is associated a USS/UTM identifier that matches the USS/UTM id from the location request and sends the UAV location information to the USS/UTM accordingly.

Alternatively, the AMF may perform filtering on the UEs in the given area such as to select only UEs that are UAVs served by the requesting USS/UTM (assuming AMF has stored USS/UTM identifier as described in 6.X.2.1 or UAVF provides it to AMF in the location request).

6.12.3 Solution evaluation

This solution complements solution#25 in TR 23.754 adopted for normative work for UAV location tracking.

This solution addresses Key Issue #5 requirement on linkability and trackability attacks on UAV by preventing the exposure of sensitive UAV information to unauthorized entities during location tracking procedures. UAV information provided in response to location tracking request includes one or more UAV identitifier (3GPP UAV ID, CAA-level UAV ID) and geographical location.

The "fake USS/UTM" issue from Key Issue #1 is addressed as follows: USS/UTM is authenticated by UAVF (UAS NF) using aviation domain provisioned certificates. USS/UTM address is provided by UE or by a trusted resolution function (using the CAA-level UAV ID provided by the UAV).

This solution addresses Key Issue #4 requirement on location tracking authorization by checking that the USS/UTM making the location request is authorized for such request (i.e., has been associated with the UAV during UUAA). For location tracking of a set of UAVs in a given geographical area (i.e., "uknown" UAV tracking mode), the AMF and/or UAVF (aka UAS NF) performs a filtering of the relevant UAVs in the area to only send information about UAVs that have been associated with the USS/UTM.

6.13 Solution #13: Authorisation of UAV/UAVC when connected to EPS

6.13.1 Solution overview

This solution addresses Key issues #1: and Key issue #2: Pairing authorization for UAV and UAVC

6.13.2 Solution details

6.13.2.1 General

The solution uses a UAV Flight Enablement Subsystem (UFES) as a single point of contact between the PLMN and USS/UTM in order to limit the impact on the 3GPP system, although it is not strictly necessary for authentication and authorisation solution to work. The authentication and authorisation procedures are shown when connected to EPS and the authentication/authorisation takes place during PDN connection establishment. The procedure in 6.X.2.2 are used to authenticate and authorize a UAV.

6.13.2.2 Authentication and authorisation

Figure 6.13.2.2-1 shows how the UAV can be authenticated and authorised by the USS/UTM when connected to EPS.

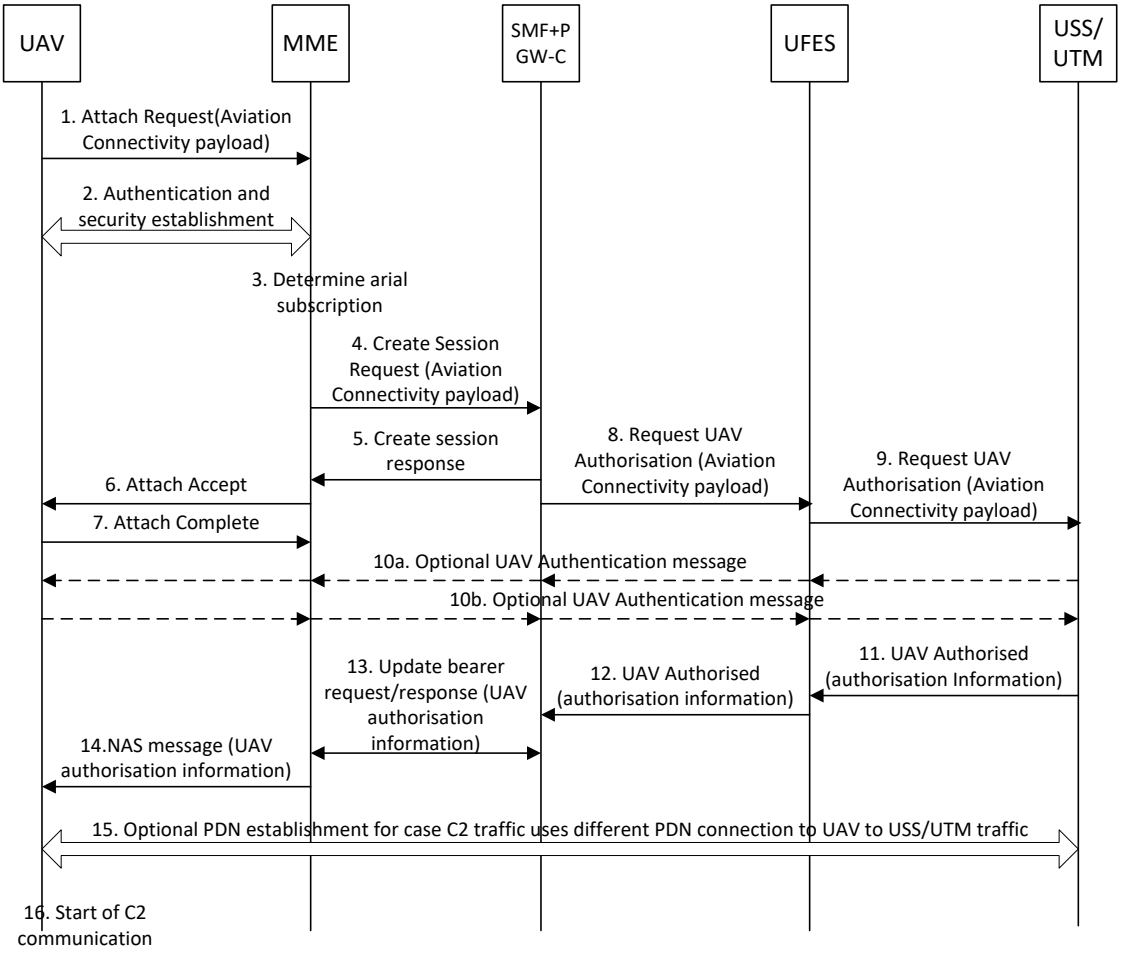


Figure 6.13.2.2-1: Authentication and authorisation of a UAV connection to EPS

The steps are as follows:

1. The UAV sends an Attach Request to the MME. The UAV includes the Aviation Connectivity payload which contains the allocated CAA-Level UAV ID and flight/pairing information in the message.

2. The MME authenticates the UAV and establishes the security.

3. The MME determines the subscription is an aerial subscription and selects the SMF+PGW-C to establish the default bearer.

4. The MME sends a Create Session Request message to the SMF+PGW-C. The message includes the Aviation Connectivity payload.

5. The SMF+PGW-C responds with a Create Session Response. At this point the UAV is restricted from sending user plane traffic.

6. The MME sends an Attach Accept message to the UAV.

7. The UAV responds with an Attach Complete message to the MME.

8. The SMF+PGW-C requests a UAV authentication and authorisation from the UFES and includes the Aviation Connectivity payload in the request.

9. The UFES forwards the information to the USS/UTM. Only authorised USS/UTMs will be used in order to ensure only legitimate entities can provide authorisation for UAVs.

10a. and 10b. There can be several round trips required for authentication of the UAV by the USS/UTM depending on the authentication method used by the USS/UTM and UAV. The authentication method and the content of messages used for authentication are out of scope of 3GPP. The content of the messages is carried in containers that are passed along and not processed by the entities between the UAV and USS/UTM.

11. On a successful authentication and authorisation of the UAV, the USS/UTM stores the 3GPP UAV ID with the CAA-level UAV ID. The USS/UTM informs the UFES that the UAV has been successfully authenticated and authorised by the USS/UTM. The USS/UTM includes authorisation information for both the network and the UAV.

12. The UFES further informs the SMF+PGW-C that the UAV has been successfully authenticated and authorised by the USS/UTM. The UFES passes the received authorisation information onto the SMF+PGW-C. The SMF+PGW-C stores the network authorisation information as part of the UE context. The network authorisation information further contains the information whether USS/UTM authentication and authorisation is required during future registrations and whether to allow UE to establish PDN connections(s) dedicated for the UAS service with or without further USS/UTM authentication and authorisation. The network part of the authorisation data contain authorisation information applicable to existing PDN connections, which influence SMF+PGW-C decisions for the traffic on these connections. For example, the information may indicate to disable all connectivity of the UAV except for the connectivity to USS/UTM.

13. The SMF+PGW-C sends the Update Bearer Request message to the MME and include the UAV authorisation information. The MME responds with the Update Bearer Response message. The SMF+PGW-C also set the traffic filters to allow traffic based on the received authorisation information.

14. The MME passes the UAV authorisation information to the UAV to inform the UAV that the authorisation was successful. The UAV authorisation information contains any needed aviation information, e.g. a new CAA-level UAV ID.

15. If using different PDN connections for C2 traffic, the UAV triggers a PDN connection set-up procedure which may include a further UAV authentication and authorisation.

16. C2 traffic can start to pass between UAV and UAVC,

6.13.2.3 Revocation

Figure 6.13.2.3-1 shows how the authorisation for some connectivity can be revoked.

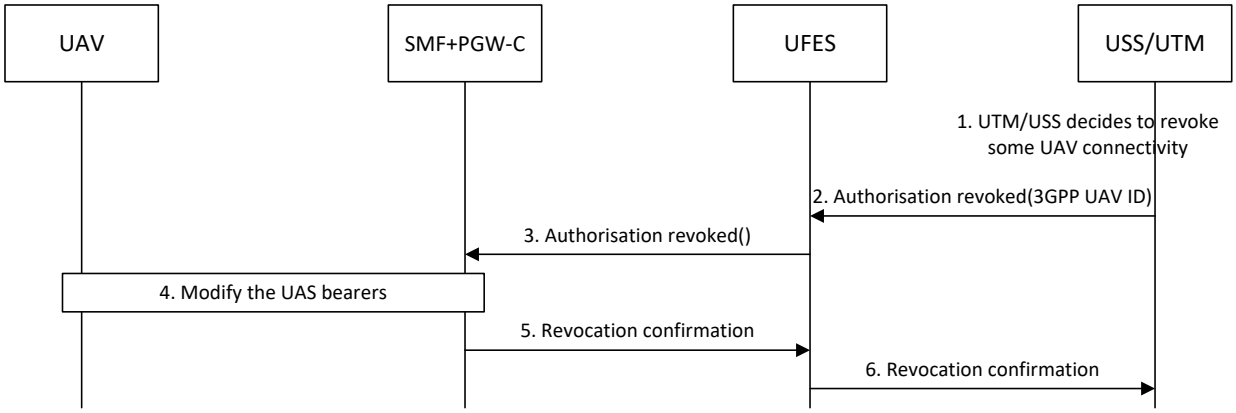


Figure 6.13.2.3-1: UAV connectivity revocation

1. The USS/UTM decides to revoke the UAV's authorisation for some connectivity.

2. The USS/UTM sends an Authorisation Revoke request to the UFES including the 3GPP UAV ID and details of the connectivity (e.g. UAV-C's IP address) to be revoked (e.g. a pairing with a UAV-C is no longer needed).

3. The UFES passes the Authorisation Revoke request to the relevant SMF+PGW-C(s) which are selected based on the details of the connectivity to be revoked.

NOTE: SMF+PGW-C selection details are left for the normative phase.

4. The SMF+PGW-C removes the connectivity of the UAV based on the received details (e.g. prevents the UAV from communicating with the UAV-C).

5. The SMF+PGW-C confirms to the UFES that the revocation of connectivity has happened.

6. The UFES confirms to the USS/UTM that the revocation of connectivity has happened.

6.13.3 Solution evaluation

This solution addresses key issues #1 and key issue #2 for a UAV connected to a 4G core network. The solution provides a method for the USS/UTM to authenticate and authorise a UAV before the UAV can access UAS services from the 3GPP system and in particular before a connection between a paired UAV and UAV-C can be enabled. The solution also provides a method of revoking the authorisation and ensure only legitimate USS/UTMs can provide the authorisations for UAVs.

6.14 Solution #14: Authorisation of UAV/UAVC pairing when connected to 5GS

6.14.1 Solution overview

This solution addresses Key issue #2: Pairing authorization for UAV and UAVC.

6.14.2 Solution details

6.14.2.1 General

The solution uses a UAV Flight Enablement Subsystem (UFES) as a single point of contact between the PLMN and USS/UTM in order to limit the impact on the 3GPP system, although it is not strictly necessary for authentication and authorisation solution to work. The authentication and authorisation procedures are shown when connected to 5GS and the authentication/authorisation takes place during PDU connection establishment. The procedure in 6.X.2.2 are used to authenticate and authorize a UAV to allow pairing with a UAVC.

6.14.2.2 Pairing authentication and authorisation

Figure 6.14.2.2-1 shows how the UAV can be authenticated and authorised by the USS/UTM to allow a connection with a paired UAVC. The flows assume that the UAV has already connected to 5GS and been authorised to act as a UAV (see for example solution #6.8).

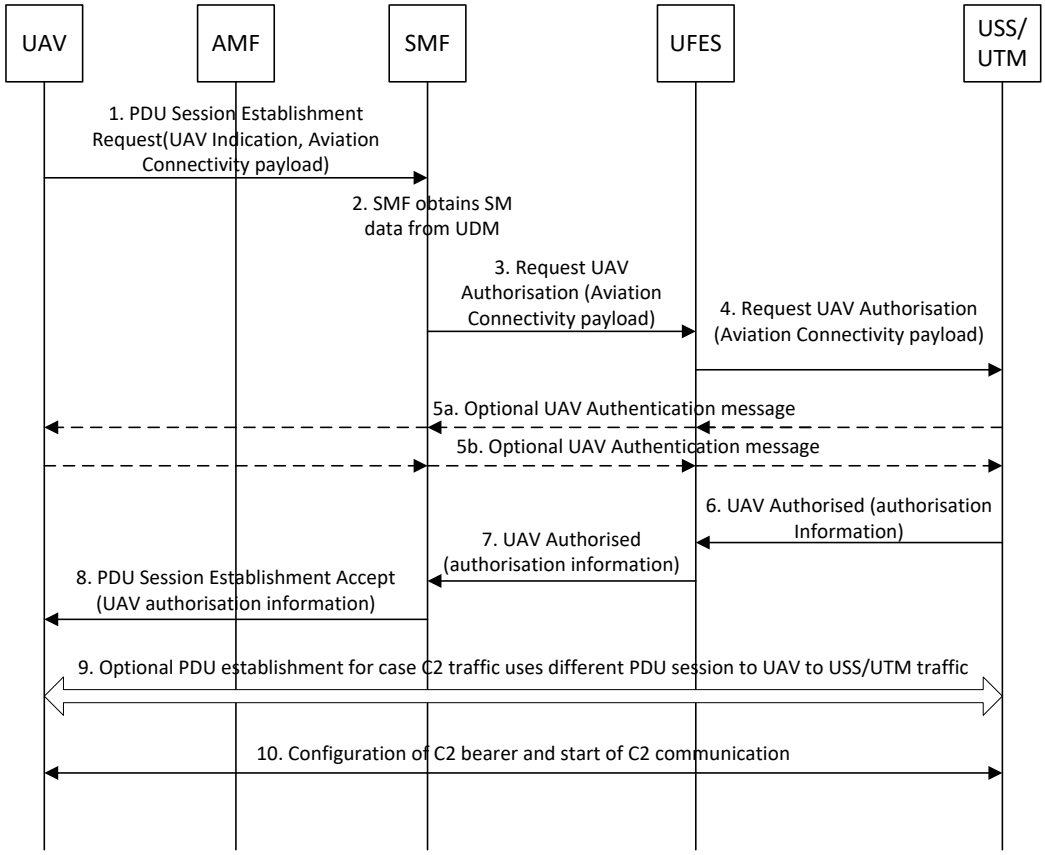


Figure 6.14.2.2-1: Authentication and authorisation of a connection between a UAV and UAVC

In the following steps, if multiple PDU sessions are established for UAV to USS/UTM and UAV to UAVC communications, respectively, the first PDU session established is for UAV to USS communications. In case of multiple PDU sessions, the UAV provides the information related to authorizing the pairing between the UAV and UAVC only during the establishment of the PDU session for UAV to UAVC communications.

The steps are as follows:

1. The UAV sends a PDU Session Establishment Request to the SMF with an indication that the PDU session is for UAV operation. The UAV also include the Aviation Connectivity payload which contains the allocated CAA-Level UAV ID and flight/pairing information.

2. The SMF obtains the SM information from the UDM.

3. The SMF requests a UAV authentication and authorisation from the UFES and includes the Aviation Connectivity payload in the request.

4. The UFES forwards the information to the USS/UTM.

5a. and 5b. There can be several round trips required for authentication of the UAV by the USS/UTM depending on the authentication method used by the USS/UTM and UAV. The authentication method and the content of messages used for authentication are out of scope of 3GPP. The content of the messages is carried in containers that are passed along and not processed by the entities between the UAV and USS/UTM.

6. On a successful authentication and authorisation of the UAV, the USS/UTM stores the 3GPP UAV ID with the CAA-level UAV ID. The UTMS/USS informs the UFES that the UAV has been successfully authenticated and authorised by the USS/UTM. The USS/UTM includes authorisation information for both the network and the UAV.

7. The UFES further informs the SMF that the UAV has been successfully authenticated and authorised by the USS/UTM. The UFES passes the received authorisation information onto the SMF. The SMF stores the network authorisation information as part of the UE context. The network authorisation information further contains the information whether USS/UTM authentication and authorisation is required during future registrations and whether to allow UE to establish PDU session(s) dedicated for the UAS service with or without further USS/UTM authentication and authorisation. The network part of the authorisation data contain authorisation information applicable to existing

PDU sessions, which influence SMF decisions for the traffic of PDU sessions. For example, the information may indicate to disable all connectivity of the UAV except for the connectivity to USS/UTM.

8. The SMF triggers a PDU Session Establishment Accept message to the UE. The message procedure contains the UAV authorisation information. Part of the contents of the UAV authorisation information may be passed to the UAV without modification by any entities between USS/UTM and UAV. The UAV authorisation information contains any needed aviation information, e.g. a new CAA-level UAV ID.

9. If multiple PDU sessions are used, then the UE triggers a PDU establishment for C2 traffic. This follows steps 1 to 8. In the case of C2 traffic, the USS/UTM provides the necessary information on the UAV-C to allow the network to set the traffic filters in the PDU session to allow connectivity to the UAV-C.

10. The SMF establishes the necessary flow(s) to enable the communication between the UAV and UAVC and C2 traffic can be sent between the UAV and UAVC.

6.14.2.3 Revocation

Figure 6.14.2.3-1 shows how the authorisation for some connectivity can be revoked.

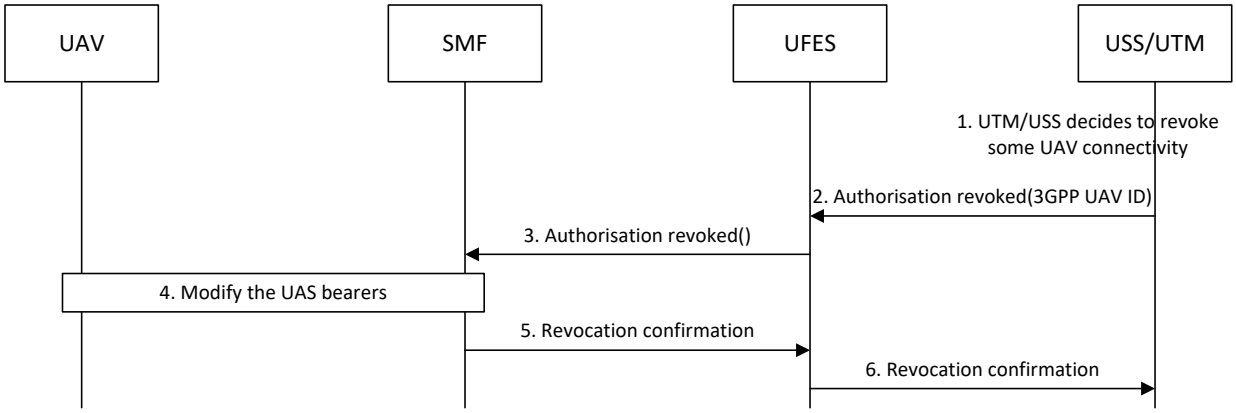


Figure 6.14.2.3-1: UAV connectivity revocation

1. The USS/UTM decides to revoke the UAV's authorisation for some connectivity.

2. The USS/UTM sends an Authorisation Revoke request to the UFES including the 3GPP UAV ID and details of the connectivity (e.g. UAV-C's IP address) to be revoked (e.g. a pairing with a UAV-C is no longer needed). Before proceeding with the revocation, the UFES checks that the USS/UTM was the one that authorised the UAV.

3. The UFES passes the Authorisation Revoke request to the relevant SMF(s) which are selected based on the details of the connectivity to be revoked.

NOTE: SMF selection details are left for the normative phase.

4. The SMF removes the connectivity of the UAV based on the received details (e.g. prevents the UAV from communicating with the UAV-C). This is performed using PDU session release (e.g. when removing one of multiple PDU sessions) or PDU session modification (e.g. when restricting connectivity in the single PDU case).

5. The SMF confirms to the UFES that the revocation of connectivity has happened.

6. The UFES confirms to the USS/UTM that the revocation of connectivity has happened.

6.14.3 Solution evaluation

This solution addresses key issue #2 for a UAV connected to a 5G core network. The solution provides a method for the USS/UTM to authenticate and authorise a UAV before the UAV can obtain connectivity from the 3GPP system and in particular before a connection between a paired UAV and UAV-C can be enabled. The solution also provides a method or revoking the authorisation.

6.15 Solution #15: UAV and UAV-C Pairing Authorization and Security Aspects

6.15.1 Solution overview

This solution address key issues #2 and #7. Further, the solution takes into account the following SA2 TR 23.754 Clause 4.2 Architectural Assumptions.

- For networked UAV controllers and non-networked UAV controllers, pairing between the UAV and the UAV controller for the use of UAV3 or UAV5 may be at least authorized, or even authenticated. The pairing authorization/authentication, when performed, is authorized by the USS/UTM, not by the 3GPP system. The 3GPP system enables such authorization process. The result of such authorization/authentication are made known to the MNO in order to enable the USS/UTM to enable the connectivity between the UAV and the UAV controller.

The solution enables UAV and UAV-C pairing authorization to ensure only authorized UAV and UAV-C to establish data connection for C2 communication between them. Further the solution also enables UAV and UAV-C pairing revocation when determined and notified by the USS/UTM.

6.15.2 Solution details

The authorization of UAV and UAV-C pairing can be performed by the USS/UTM (after a successful primary authentication and during/after a successful UAS authentication) when a UAV initiates a PDU session establishment or when the UAV modifies the existing PDU session to set up C2 connection with the UAV-C for enabling the UAS service as shown in Figure 6.15.2-1. At this step, it is considered that UAV and UAV-C has already performed successful UAS registration with the USS/UTM (and has UAS authorization and security information provided by the USS/UTM). The UAV shall include Pairing authorization request information containing UAV-C ID, Auth Token, UAS ID, Security context ID in addition to its CAA-level UAV ID in the PDU session establishment request message (or in PDU session modification request) to SMF along with the UAV operation request and SMF can send the UAV operation Request along with the received Pairing authorization request information to the UFES and the UFES forwards the same to the USS/UTM. UAV operation Request procedure can be based on agreements from SA2 23.754. The USS/UTM on receiving the Pairing authorization request information along with UAV operation request can perform the UAV and UAV-C pairing authorization and session security set up. Pairing authorization can also be referred C2 Association authorization. The solution considers that, the UAV-C information (i.e., a UAV-C ID) with which the UAV can form an UAS can be available in the USS and it can also be prepositioned to the UAV along with the CAA-level UAV ID provisioning (out of 3GPP scope) as a precondition.

UAV and UAV-C pairing authorization and session security set up procedure is described as follows.

As a precondition, the UAV and UAV-C is registered to the 3GPP network and both UAV and UAV-C has successfully performed UAS Authentication and authorization with the USS/UTM and established a PDU Session with the USS/UTM. Alternatively, the UAV-C may be connected to the USS/UTM over internet.

1. The UAV sends to the AMF, a PDU Session establishment Request with Pairing Authorization Request Information. Pairing Authorization Request Information includes UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token (the one received during successful UAA from USS/UTM), UAS Security Context Identifier (the one received during the successful UAA from USS/UTM to uniquely identify the UAS security context information established between UAV and USS/UTM).

2. The AMF on receiving the PDU Session establishment Request with Pairing Authorization Request Information, checks if the UAV-ID is authorized to request pairing authorization based on the locally stored UAS authentication and authorization results, authorization information (Token) and UAV-C ID (if available). If both the received Pairing authorization request information and locally stored information matches, the AMF considers the check as successful and perform step 3. If the AMF does not find any UAS authentication results or if the authentication result or authorization information locally stored doesn't match with the received authorization information, then the AMF triggers UAA as in Solution#7.

3. The AMF sends Nsmf_PDUSession_CreateSMContext Request to the SMF with the received Pairing Authorization Request Information which includes UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token, UAS Security Context Identifier and 3GPP UAV ID (i.e., GPSI).

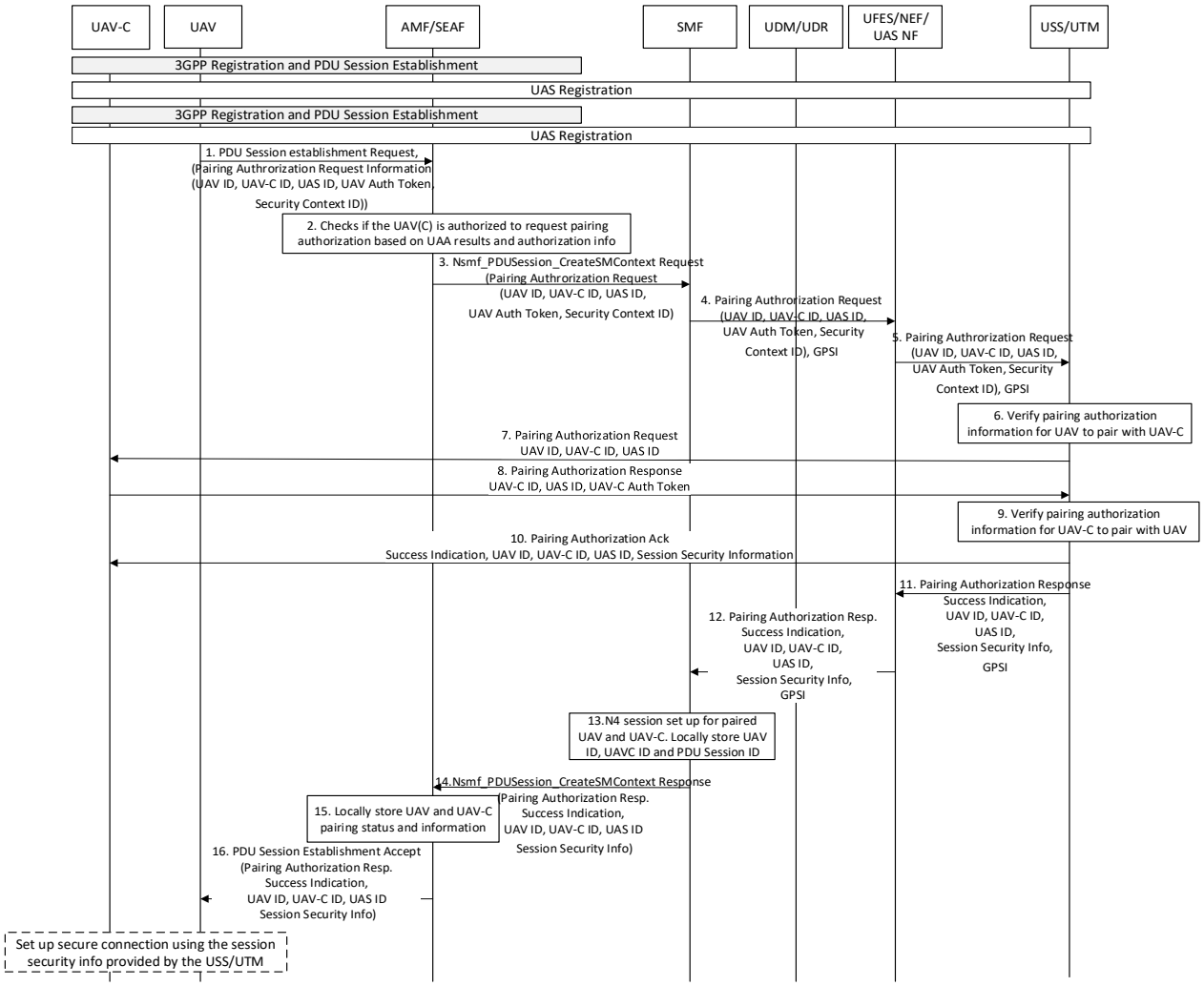


Figure 6.15.2-1: UAV and UAV-C pairing authorization

4. The SMF sends the received Pairing Authorization Request to the UFES (in a service operation message) with UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token, UAS Security Context Identifier along with GPSI and UAV IP address (based on TR 23.754).

5. The UFES sends the received Pairing Authorization Request to the USS/UTM (in a service operation message) with UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token, UAS Security Context Identifier along with GPSI and UAV IP address.

6. The USS/UTM verifies the information received in the Pairing Authorization Request with the locally stored information and if the verification is successful, the USS/UTM determines to authorize pairing for the UAV.

Optionally Step 7-10 can be skipped and only step 10 is performed if the UAV-C is connected to the USS/UTM over internet.

7. The USS/UTM sends to the UAV-C identified with the UAV-C ID (via the 3GPP network or over internet) a Pairing Authorization Request, which includes UAV ID, UAV-C ID and UAS ID.

8. The UAV-C in response sends to USS/UTM, a Pairing Authorization Response message which includes UAV-C ID, UAS ID, UAV-C IP address, and UAV-C Authorization Token.

9. The USS/UTM verifies the information such as UAV-C ID, UAS ID, and UAV-C Authorization Token received in the Pairing Authorization Response message by checking with the locally stored information. If the received authorization information match with the locally stored information, the USS/UTM considers the UAV-C pairing authorization as successful.

10. The USS/UTM sends a Pairing Authorization Acknowledgement/Notification message to the UAV-C, which contains Pairing Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information (i.e., to set up session security), UAV IP address.

11. Further the USS/UTM sends a Pairing Authorization Response/Accept message to the UFES in response to receiving step 5. The Pairing Authorization Response contains Pairing Success indication, UAV ID, UAV-C ID, UAS ID, Session Security Information, GPSI, and UAV-C IP address.

12. The UFES sends the received Pairing Authorization Response to the SMF, which contains Pairing Success indication, UAV ID, UAV-C ID, UAS ID, Session Security Information, GPSI and UAV-C IP address.

13. The SMF locally stores the information received in the Pairing Authorization Response as part of pairing authorization status information. Further performs N4 session set up for the authorized pair of UAV and UAV-C.

14. The SMF sends Nsmf_PDUSession_CreateSMContext Response to the AMF with the received Pairing Authorization Response Information which includes Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information.

15. The AMF optionally stores the UAV ID and UAV-C ID along with the pairing authorization status and UAS ID.

16. The AMF sends a PDU Session Establishment Accept message to the UAV over the N1 interface and the PDU Session Establishment Accept message includes the received Authorization Response Information which includes Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information.

The UAV and UAV-C uses the received session security information to set up a secure connection between UAV and UAV-C for the C2 connection.

In case of modifying the existing PDU session during pairing authorization, the steps 1-3 and steps 14-16 will use PDU session modification related message (i.e., PDU session modification request/response message instead of PDU session initiation request/response and PDU session update SM context message instead of PDU session create SM context message accordingly.). The SMF performs the configuration of the PDU Session accordingly to enforce pairing based on the received UAV-C authorization Pairing Authorization Response.

Pairing Authorization Revocation:

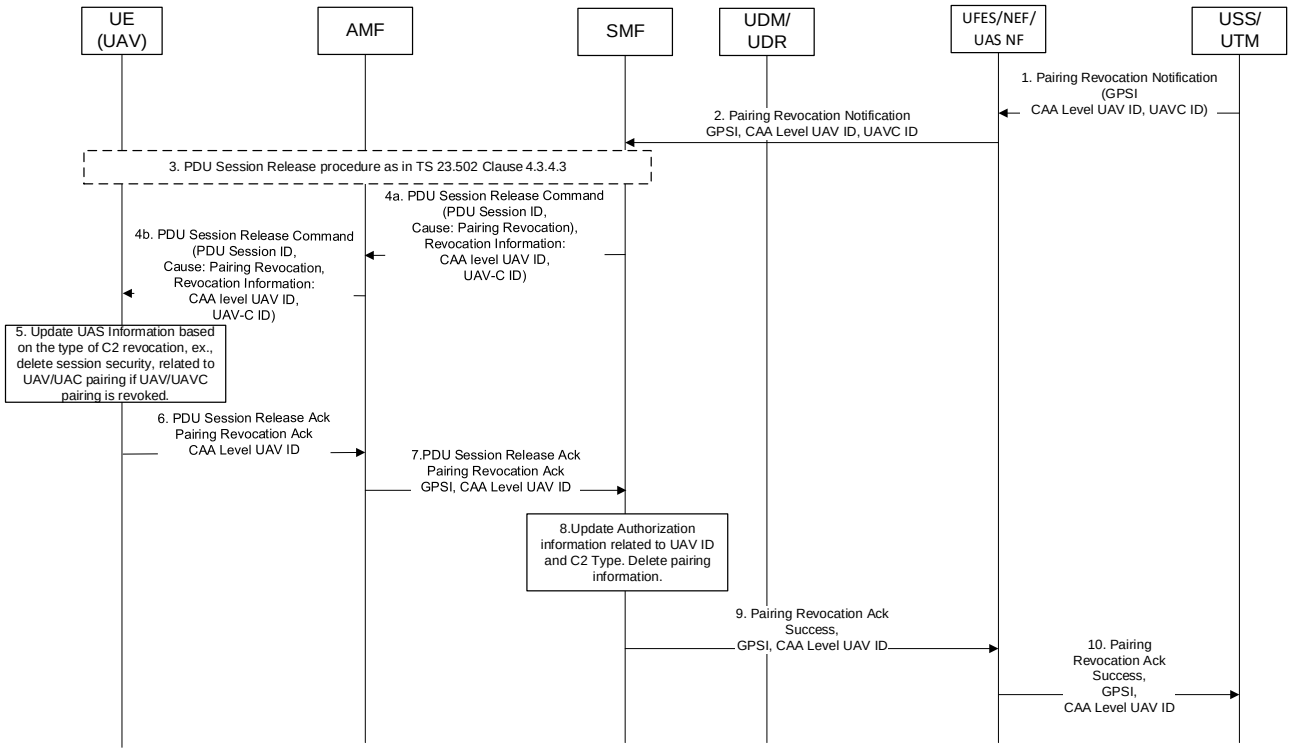


Figure 6.15.2-2: UAV and UAV-C pairing authorization revocation

UAV and UAV-C pairing revocation is shown in Figure 6.15.2-2 and the steps involved in the pairing revocation is described as follows.

1. The USS/UTM when it determines to revoke UAV/UAV-C pairing (also known as C2 pairing or C2 association), the USS/UTM sends a Pairing Revocation Notification to the UFES with the GPSI, CAA Level UAV ID and UAV-C ID.

2. The UFES uses the Nudm_UECM_Get Request/Response service operation to fetch the serving SMF information corresponding to the GPSI. Further, the UFES sends the received Pairing Revocation Notification message to the serving SMF, which contains GPSI, CAA Level UAV ID, and UAV-C ID.

3. The SMF on receiving the Pairing Revocation Notification, checks if there is any active PDU Session corresponding to the indicated CAA level UAV ID with a UAV-C ID. If there is any active PDU Session, the SMF performs PDU Session release procedure for the associated PDU Session IDs using the existing procedure in TS 23.502 Clause 4.3.4.3. with the following adaptations.

4a. The SMF sends a PDU Session Release command to the AMF including the PDU Session ID along with a suitable cause value and a pairing revocation information containing CAA level UAV ID and UAV-C ID based on the received pairing revocation notification.

4b. The AMF forwards the PDU Session Release command to the UAV which includes PDU Session ID, with a suitable cause value, and a pairing revocation information containing CAA level UAV ID and UAV-C ID.

5. The UAV on receiving the PDU Session Release command with a pairing revocation information will delete the locally stored pairing authorization information (token, lifetime, identifiers or any related information) and associated security information for the UAV and UAV-C pairing indicated in the revocation information.

6. The UAV sends a PDU Session Release acknowledgement message to the AMF by including the Pairing Revocation Ack indication and CAA Level UAV ID.

7. The AMF deletes locally stored pairing information (such as pairing authorization information and paired UAV and UAV-C IDs if available) for the UAV corresponding to its CAA Level UAV ID. Further the AMF sends a PDU Session Release Acknowledgement message to the SMF with the GPSI, received Pairing Revocation Ack indication and CAA Level UAV ID.

9. The SMF on receiving the Pairing Revocation Ack indication deletes locally stored pairing information (such as pairing authorization information and paired UAV and UAV-C IDs) if available for the UAV corresponding to its CAA Level UAV ID. Further, the SMF sends a Pairing Revocation Acknowledgement to the UFES with the received GPSI, Success Indication, and CAA Level UAV ID.

10. The UFES forwards the received Pairing Revocation Acknowledgement to the USS/UTM with the received Success Indication, GPSI and CAA Level UAV ID.

Pairing Revocation related to UAV-Controller (UAV-C) Change:

NOTE 1: SA2 Conclusion specifies that, 'For UAVC replacement, solution #27 may be taken in addition to improve KI#6.'. Therefore, the adaptation described in this section can be used for UAVC replacement when required.

1. The UAV is communicating with UAV-C1 after a successful pairing authorization.

2. The USS/UTM determines to change the UAV-C for a UAV (the determination aspects at USS/UTM are out of 3GPP scope) and sends to SMF via UFES a UAV Operation update message with 3GPP UAV ID, new authorization data (i.e., CAA level UAV ID, new UAV-C2 info (example., ID and IP address), session security information and new UAS ID if any), pairing authorization indication and Cause indicating UAV-C Change.

NOTE 2: SA2 defines the content of UAV and UAVC pairing information, e.g. 3GPP UAV IDs and corresponding IP addresses and how the IP addresses of UAV and UAVC are available to the USS/UTM is up to SA2 as specified in Solution#27.

3. The SMF initiates PDU session modification procedure (via the serving AMF with the UAV) by sending to AMF, N1 SM container with PDU session Modification command along with the received Pairing authorization indication, new authorization data and a suitable cause value based on the received UAV-C change indication.

4. The AMF forwards the PDU session modification command message to the UAV along with the received Pairing authorization indication, new authorization data and a suitable cause value based on UAV-C change indication.

5. The UAV updates the pairing information based on the received new authorization data and sends a PDU Session Modification Command Ack to AMF. The AMF can update the locally stored pairing information if any (such as paired

UAV and UAV-C information, authorization status based on new authorization data received) and forwards the received PDU Session Modification Command Ack to SMF. The SMF can also update the locally stored pairing information if any and updates N4 session of the UPF(s) that are involved by the PDU Session Modification for the new authorized pair of UAV and new UAV-C2 (based on UAV and UAV-C information received from USS/UTM).

6. The UAV communicates with the UAV-C2.

Applicability to EPS:

The UAV/UAV-C (i.e., C2) Pairing authorization and Revocation procedure described in this section can be applicable to EPS, with the adaptation of using MME, SMF+PGW-C, UPF+PGW-U and HSS+UDM respectively. 3GPP NF/UFES can act as a UAS NF or UAS control function in the 3GPP network which can be a standalone network function, or a service offered by the SCEF in the EPS. The message name used in EPS procedure can be aligned with SA2 where required during the normative work. The UAV and UAV-C pairing authorization when connected to EPS is described as follows.

1. The UAV sends to MME, a PDN connection Request with Pairing Authorization Request Information. Pairing Authorization Request Information includes UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token (the one received during successful UAA from USS/UTM), UAS Security Context Identifier (the one received during the successful UAA from USS/UTM to uniquely identify the UAS security context information established between UAV and USS/UTM).

2. The MME on receiving the PDN connectivity Request with Pairing Authorization Request Information, checks if the UAV-ID is authorized to request pairing authorization based on the locally stored UAS authentication and authorization results, authorization information (Token) and UAV-C ID (if available). If both the received Pairing authorization request information and locally stored information matches, the MME considers the check as successful and perform step 3. If the MME does not find any UAS authentication results or if the authentication result or authorization information locally stored doesn't match with the received authorization information, then the AMF triggers UAA as in Solution#7.

3. The MME sends Create Session Request to the SMF+PGW-C via S-GW with the received Pairing Authorization Request Information which includes UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token, UAS Security Context Identifier and 3GPP UAV ID (i.e., an external identifier).

4. The SMF+PGW-C sends the received Pairing Authorization Request to the UFES which contains UAV ID, Target UAV-C ID, UAS ID, UAV Authorization Token, UAS Security Context Identifier along with 3GPP UAV ID and UAV IP address (based on TR 23.754).

5. The UFES sends the received Pairing Authorization Request to the USS/UTM.

6-10. Steps 6-10 can be performed as described for 5GS.

11. Further the USS/UTM sends a Pairing Authorization Response/Accept message to the UFES in response to receiving step 5. The Pairing Authorization Response contains Pairing Success indication, UAV ID, UAV-C ID, UAS ID, Session Security Information, 3GPP UAV ID, and UAV-C IP address.

12. The UFES sends the received Pairing Authorization Response to the SMF+PGW-C.

13. The SMF+PGW-C locally stores the information received in the Pairing Authorization Response as part of pairing authorization status information. Further performs N4 session set up for the authorized pair of UAV and UAV-C.

14. The SMF+PGW-C sends Create Session Response to the MME via S-GW, with the received Pairing Authorization Response Information which includes Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information.

15. The MME optionally stores the UAV ID and UAV-C ID along with the pairing authorization status and UAS ID.

16. The MME sends a PDN Connection Accept message to the UAV over the NAS and the PDN Connection Accept message includes the received Authorization Response Information which includes Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information.

The UAV and UAV-C can use the received session security information to set up a secure connection between UAV and UAV-C for the C2 connection.

The UAV and UAV-C pairing revocation can be applicable to EPS as described below.

The USS/UTM when it determines to revoke UAV/UAV-C pairing (also known as C2 pairing or C2 association), the USS/UTM sends a Pairing Revocation Notification to the UFES with the 3GPP UAV ID (i.e., an external identifier), CAA Level UAV ID and UAV-C ID. The UFES sends the received Pairing Revocation Notification message to the SMF+PGW-C and a PDN connection disconnection and bearer deactivation can be initiated based on TR 23.754 and TS 23.401 accordingly. The Delete Session/bearer Request can be sent by SMF+PGW-C to MME via S-GW with a suitable cause value and a pairing revocation information containing CAA level UAV ID and UAV-C ID based on the received pairing revocation notification. During bearer deactivation, the MME can send to the UAV, a suitable cause value and a pairing revocation information containing CAA level UAV ID and UAV-C ID. The UAV on receiving the pairing revocation information will delete the locally stored pairing authorization information and security information for the UAV and UAV-C pairing and releases all resources corresponding to the PDN connection. The UAV sends in response, a pairing revocation acknowledgement and CAA level UAV ID to the MME. The MME sends a PDN connection Release Acknowledgement (example., in a delete bearer response) to SMF+PGW-C via SGW with the external ID, Pairing Revocation Ack indication and CAA Level UAV ID. The SMF+PGW-C on receiving the Pairing Revocation Ack indication deletes locally stored pairing information (such as pairing authorization information and paired UAV and UAV-C IDs). Further, the SMF+PGW-C sends a Pairing Revocation Acknowledgement to the UFES with the received 3GPP UAV ID, Success Indication, and CAA Level UAV ID. The UFES forwards the received Pairing Revocation Acknowledgement to the USS/UTM with the received Success Indication, 3GPP UAV ID and CAA Level UAV ID. In case of UAV change, an authorization indication, new authorization data with cause as UAV change can be notified by the USS/UTM to the UFES. The PDN connection modification can be triggered by the SMF+PGW-C and the UAV can be notified with an authorization indication, new authorization data with cause as UAV change to allow the UAV to update the pairing authorization information during the PDN connection modification. The UAV updates the pairing information based on the received new authorization data and sends an acknowledgement back to MME. The MME forwards the received acknowledgement to SMF+PGW-C. The SMF+PGW-C can also update the locally stored pairing information if any (such as paired UAV and UAV-C information, authorization status based on new authorization data received) and updates session that are involved by the PDN connection Modification for the new authorized pair of UAV and new UAV-C2 (based on UAV and UAV-C information received from USS/UTM).

6.15.3 Solution evaluation

AMF in 5GS and SMF+PGW-C in EPS: On receiving a pairing authorization request information, need to verify if the UAV-ID is authorized to request pairing authorization based on the locally stored UAS authentication and authorization results, authorization information (i.e., Auth Token) and UAV-C ID (if available). If there are no UAS authentication results available or if doesn't match, then triggers UAA before performing pairing authorization.

After a successful pairing authorization, receives (from USS/UTM via UFES) and forwards the Authorization Response Information with Success Indication, UAV ID, UAV-C ID, UAS ID, and Session Security Information to the UAV, to allow session security set up between the paired UAV and UAVC. Also stores the UAV ID and UAV-C ID along with the pairing authorization status and UAS ID to enable handling of paired connections later (example. during pairing revocation and UAVC change).

UE: On a PDU session establishment related to C2, sends Pairing Authorization Request Information which includes UAS ID, UAV Auth Token, and UAS Security Context Identifier.

On a PDU session or PDN connection release related to a pairing revocation requested by the USS/UTM (via UFES), the UAV is notified (via AMF/MME accordingly) with a Pairing Revocation Indication and pairing revocation information to enable UAV to delete any pairing authorization information locally stored.

On a PDU session/PDN connection modification related to a UAVC change requested by the USS/UTM (via UFES), the UAV is notified (via AMF and MME accordingly) with a UAVC Change and new authorization information to enable UAV to update any pairing authorization information locally stored.6.16

Solution #16: Preventing malicious revocation from unauthorised UTM/USS

6.16.1 Solution overview

This solution proposes to address the fake UTM/USS issue in KI#1. Unauthorised UTM/USS, including fake UTM/USS and competitor UTM/USS, may perform malicious UAV service revocation due to the lack of authorisation checking by the 3GPP network, the contribution provides a solution to prevent the malicious revocation sent by the unauthorised UTM/USS.

According to the conclusion in TR 23.754 [3], the UTM/USS shows the 3GPP UAV ID (i.e. GPSI) to invoke MNO services and to revoke authentication & authorisation. However an unauthorised UTM/USS may perform malicious revocation to 3GPP network by sending 3GPP UAV ID captured from other places (e.g. the same 3GPP UAV ID is reused for multiple UTM/USSs, or eavesdropping on the GPSIs which are sent out from 3GPP network). To prevent the above attack, this solution allows the UAV-NF to check the revocation request is sent from the serving UTM/USS of the UAV (i.e. the authorised UTM/USS).

6.16.2 Solution details

Upon a successful USS UAV Authentication and Authorisation (UUAA) procedure between UAV and UTM/USS, the UAV-NF (a.k.a UAVF or UFES as specified in TR 23.754 [3]) stores a UUAA identity mapping between the 3GPP UAV ID and the UTM/USS identifier. Upon a successful pairing authorisation procedure, the UAV-NF stores a pairing identity mapping between the 3GPP UAV ID and the UTM/USS identifier.

During either UUAA revocation or pairing revocation, the UTM/USS uses 3GPP UAV ID to invoke the corresponding revocation, the revocation request message sent from UTM/USS includes its UTM/USS identifier. The UAV-NF verifies the revocation request by checking the 3GPP UAV ID and UTM/USS identifier match the previously maintained mapping relationships accordingly (either UUAA ID mapping or pairing ID mapping). The UAV-NF stops the subsequent revocation procedures if the 3GPP UAV ID and the UTM/USS identifier sent from the UTM/USS do not match the previously maintained mapping relationships.

6.16.3 Solution evaluation

This solution addresses the fake UTM/USS issue in Key Issue #1 by introducing additional checks at UAV-NF (aka UAVF or UFES) to avoid unauthorised revocation (UUAA revocation or pairing revocation). This solution requires UAV-NF to associate the 3GPP UAV ID with the UTM/USS identifier after UUAA procedures. The UTM/USS is required to send both 3GPP UAV ID and UTM/USS identifier to UAV-NF to perform revocation(s). The UAV-NF needs to verify the associated identities provided by the UTM/USS before the rest revocation procedures.

Editor's Note: This below provides a generic set of headings for a new solution and need to be deleted before the TR goes for approval

6.X Solution #X: <Solution name>

6.X.1 Solution overview

6.X.2 Solution details

6.X.3 Solution evaluation

7 Conclusions

7.1 Conclusions for KI#1

UAV Authentication and Authorization (UAA) is recommended for the normative work based on the following solutions and principles:

NOTE: The agreement for normative work is on key common principles and not on the other details of the solutions.

- UAA is performed in 5G systems or EPS.

- UAA is performed between UAV and USS/UTM after Primary Authentication
- Revocation of UAV is initiated by USS/UTM using the 3GPP UAV ID
- UAA is performed either optionally during registration (5G solutions #1, #3, #7, #10 as basis) or during PDU session establishment (5G solution #5 as basis)
- USS/UTM is authorised to perform UAV authorization revocation, it is verified by UAS-NF (5G solutions #16 as basis)
- For EPS: solution #13 is chosen as the basis for normative work, with similar principles above
- In UAA, CAA Level UAV ID is used to identify UAV.
- Specific authentication methods for UAA are out of scope of 3GPP, the messages used for UAA exchanged between UAV and USS/UTM are included in transparent containers.
- Security related application layer information can be transported between UAV and USS/UTM in transparent containers (the content is out of scope of 3GPP).

7.2 Conclusions for KI#2

Pairing Authorization for UAV and UAVC is recommended for the normative work based on the following solutions and principles:

NOTE: The agreement for normative work is on key common principles and not on the other details of the solutions.

- Pairing authorization is performed after successful UAA between UAV and USS/UTM
- Pairing authorization is performed during PDU session establishment/modification procedure (5G solution #5, #11, #14, #15 as bases) and enforced in the 3GPP network based on connectivity information received from USS.
- Both SMF and authorized USS/UTM may trigger pairing authorization. Authorized USS/UTM may trigger updating and revocation of pairing authorization using 3GPP UAV ID (sol#15 as base for UAV-C change)
- For EPS: solution #13 is chosen as the basis for normative work, with similar principles as for 5GS above.
- During pairing authorization procedure, CAA Level UAV ID is used to identify UAV.
- The messages used for pairing authorization that are exchanged between UAV and USS/UTM are included in transparent containers and the content is out of scope of 3GPP

7.1 Conclusions for KI#3

TBD

7.4 Conclusion on KI #4

For key issue #4 on Location information veracity and location tracking authorization:

- Solution #6, solution #8 and solution#12 are chosen as basis for normative work, based on the following key common principles:
  - The UAS NF (aka UFES) receives location request from USS/UTM which may include a 3GPP UAV ID. If authorized, UAS NF provides USS/UTM with UAV location information including the 3GPP UAV ID (GPSI).
  - To obtain UAV location information, the UAS NF uses location services (LCS) as supported by AMF/MME or GMLC. The Network-Assisted Positioning Procedure between the LMF and NG-RAN is selected for location information veracity.
  - The UAS NF ensures that the USS/UTM is authorized to track the location of a given UAV before sending the UAV location information to USS/UTM. A USS/UTM is authorised to receive the location information of a group of UAVs in a particular geographic area or of an individual UAV if it has authorised the UAV(s) for service. Furthermore, a USS/UTM can be authorised to receive the data about all UAVs in a particular geographic area.

NOTE: The agreement for normative work is on key common principles and not on the other details of the solutions.

7.5 Conclusions for KI#5

TBD

7.6 Conclusions for KI#6

TBD

7.7 Conclusions for KI#7

The following is recommended for normative work:

- The transport of security information in a transparent container between USS/UTM and UAV during PDU or PDN Session establishment/modification procedure is enabled.
- The content of security information (e.g. key material to help establish security for C2 Communications) is not in 3GPP scope.

Annex <A>:
<Informative annex title for a Technical Report>

Annex <X> (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2020-08	SA3#100-e					Incorporating S3-202088, S3-202090, S3-202095, S3-202096, S3-202111, S3-202112, S3-202113, S3-202114, S3-202127 and S3-202155	0.1.0
2020-10	SA3#100-bis-e					Incorporating S3-202345, S3-202391, S3-202690, S3-202692, S3-202702, S3-202703, S3-202704, S3-202709, S3-202722 and S3-202772	0.2.0
2020-11	SA3#101-e					Incorporating S3-203292, S3-203298, S3-203300, S3-203352, S3-203352, S3-203354, S3-203371, S3-203386, S3-203387 and S3-203390	0.3.0
2021-01	SA3#102-e					Incorporating S3-210201, S3-210202, S3-210442, S3-210443, S3-210593, S3-210594, S3-210605, S3-210615, S3-210616, S3-210617, S3-210628, S3-210629, S3-210630, S3-210686, S3-210687 and S3-210688	0.4.0
2021-03	SA3#102-e-Bis					Incorporating S3-210896, S3-211212, S3-211249, S3-211220, S3-211251, S3-211252, S3-211253, S3-211254, S3-211255, S3-211256, S3-211262, S3-211263, S3-211331 and S3-211333	0.5.0
2021-05	SA3#103-e					Incorporating S3-211627, S3-211740, S3-211776, S3-212128, S3-212181, S3-212183, S3-212184, S3-212185, S3-212211, S3-21222, S3-212244, S3-212245 and S3-212246	0.6.0