|  |  |
| --- | --- |
| 3GPP TR 33.854 V0.3.0 (2020-11) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of Unmanned Aerial Systems (UAS) (Release 17) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***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 |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Overview of Unmanned Aerial Systems (UAS) 8

5 Key issues 9

5.1 Key issue #1: UAS Authentication and Authorization 9

5.1.1 Key issue details 9

5.1.2 Threats 9

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Pairing authorization for UAV and UAVC 10

5.2.1 Key issue details 10

5.2.2 Threats 10

5.2.3 Potential Security requirements 10

5.3 Key Issue #3: TPAE Authentication and Authorization 11

5.3.1 Key issue details 11

5.3.2 Threats 11

5.3.3 Potential Security requirements 11

5.4 Key issue #4: Location Information veracity 11

5.4.1 Key issue details 11

5.4.2 Threats 12

5.4.3 Potential security requirements 12

5.5 Key issue #5: Privacy protection of UAS identities 12

5.5.1 Key issue details 12

5.5.2 Threats 13

5.5.3 Potential security requirements 13

5.6 Key issue #6: Security protection of information in remote identification and between UAV/UAVC and UTM/USS 13

5.6.1 Key issue details 13

5.6.2 Threats 14

5.6.3 Potential security requirements 14

5.7 Key issue #7: Security of Command and Control (C2) Communication 14

5.7.1 Key issue details 14

5.7.2 Threats 14

5.7.3 Potential security requirements 14

5.X Key issue #X: <Key issue name> 15

5.X.1 Key issue details 15

5.X.2 Threats 15

5.X.3 Potential security requirements 15

6 Proposed solutions 15

6.1 Solution #1: UAS Authentication and Authorization 15

6.1.1 Solution overview 15

6.1.2 Solution details 15

6.1.3 Solution evaluation 17

6.2 Solution #2: UAS Authentication and Authorization using User Plane 17

6.2.1 Solution overview 17

6.2.2 Solution details 17

6.2.3 Solution evaluation 19

6.3 Solution #3: UAV authentication and authorization by USS/UTM with AMF as authenticator 19

6.3.1 Solution overview 19

6.3.2 Solution details 19

6.3.3 Solution evaluation 21

6.4 Solution #4: UAV authentication and authorization using EAP-based PDU secondary authentication 21

6.4.1 Solution overview 21

6.4.2 Solution details 22

6.4.3 Solution evaluation 23

6.5 Solution #5: UAV authentication and authorization using API-based PDU secondary authentication 23

6.5.1 Solution overview 23

6.5.2 Solution details 23

6.5.3 Solution evaluation 25

6.6 Solution #6: Obtaining UAV location information from the PLMN 25

6.6.1 Solution overview 25

6.6.2 Solution details 25

6.6.3 Solution evaluation 26

6.7 Solution #7: UAS Authentication, Authorization and Security Aspects 26

6.7.1 Solution overview 26

6.7.2 Solution details 27

6.7.3 Solution evaluation 29

6.8 Solution #8: Using 5G location result for location information verification 29

6.8.1 Solution overview 29

6.8.2 Solution details 29

6.8.3 Solution evaluation 29

6.X Solution #X: <Solution name> 30

6.X.1 Solution overview 30

6.X.2 Solution details 30

6.X.3 Solution evaluation 30

7 Conclusions 30

Annex <A>: <Informative annex title for a Technical Report> 31

Annex <X> (informative): Change history 32

# 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

### 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.

### 5.4.3 Potential security requirements

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

## 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 to integrity and replay protections of the flight information in remote identification between UAV and TPAE/UTM/USS.

The 5G System shall provide the means to provide confidentiality, integrity and replay protections of the information exchanged (UAV/UAVC identities, UAS-specific and general exchanged information) between UAV/UAVC and USS/UTM.

Editor’s Note: It is FFS what security protection is in the scope of 3GPP.

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 system shall protect the C2 Communcation to ensure UAS Security.

Editors Note: Whether a C2 Security is in 3GPP scope or outside 3GPP Scope is FFS.

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

## 6.1 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

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



**Figure 6.1.2-1: 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. 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 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.

d. USS/UTM response with EAP messages 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

5. Based on the EAP authentication outcome, USS/UTM sends the results to AMF. 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.

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

7. AMF sends UAS registration complete message to UE. The message includes the UAS-ID and may include an indication it is for a UAV (or UAVC), if needed.

Editor's note:  Whether the UUA steps are executed within or outside the Registration procedure is FFS and in coordination with SA2

Editor's note:  Which core network function(s) (AMF, and/or others) and messaging will be used in the UAV authentication and authorization by USS/UTM procedure is FFS and in coordination with SA2

Editor's note:  How authorization revocation is supported should be marked as FFS

### 6.1.3 Solution evaluation

TBC

## 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 AF (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 AA and AA method are out of 3GPP scope.

### 6.2.2 Solution details

The authentication and authorization procedure is presented in Figure 6.2.2-1.



Figure 6.2.2-1: UAA procedure

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), etc.

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

Editor’s Note: It is FFS whether the proposed AF is a CP NF or a mixed CP+UP NF (no CP UP separation).

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 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 AA request towards the UTM/USS. The UAS AF can include information 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 AA 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. 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 4: The credentials and the method used in the UAS AA are out of 3GPP scope.

Editor’s Note: Details of what information and how it is provided by MNO during the authentication and authorization procedure between UAV/UAVC and USS/UTM are FFS.

Editor’s Note: The details of secure message exchanges between UE and USS/UTM in order to support A&A by USS/UTM (e.g. EAP or other framework/mechanism) is FFS.

7. USS/UTM sends UAS AA result to UAS AF. If the AA 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.

Editor’s Note: It is FFS whether USS/UTM is able to inform 3GPP about the action to be taken.

8. If the result of the AA 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 AA 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 address UAS communication security.

NOTE 6: This solution does not enable/support authorization of UAV and UAVC pairing.

### 6.2.3 Solution evaluation

This solution requires a new function (UAS AF).

Editor’s Note: The impacts related to introducing UAS AF is FFS.

## 6.3 Solution #3: UAV authentication and authorization by USS/UTM with AMF as authenticator

### 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 EAP-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 acts as the EAP authenticator while the USS/UTM acts as the AAA server. 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.

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 EAP-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.

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.

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

TBD

## 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 using API-based PDU secondary authentication

### 6.5.1 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 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). 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 upon successful authentication and authorization. Mutiple 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).

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

NOTE 2: How the token is generated by the USS/UTM is outside the scope of 3GPP. The USS/UTM can for example bind the token 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 from USS/UTM.

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 from network Remote ID functionality). The UE provides the CAA-level UAV ID obtained following the successful authorization by USS/UTM.

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

7. The UE establishes a secure application layer communication with the USS/UTM using the authorization token obtained previously to further obtain UAS communication configuration from USS/UTM. The USS/UTM checks the validity of the presented authorization token. If the token is valid the USS/UTM may send a request to the 5GC to authorize C2 communications for the UAV identified by its 3GPP UAV ID .

NOTE 3: The secure application layer communication between the UAV and USS/UTM is outside of the scope of 3GPP. Such application exchanges may trigger the USS/UTM to request PDU Session configuration from the 3GPP network (e.g., ACL for enforcement of pairing with UAV-C authorization). Additional details for PDU session configuration for pairing authorization are assumed to be covered in solutions for KI#2.

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

#### 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

TBD

## 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 UTM/USS.



**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 UTM/USS sends the location request to UFES to request the UAV location from network. The UTM/USS includes the relevant identity of the UAV.

Editor’s Note: More detailed information on interaction between UTM/USS and UFES (or NFs) is FFS.

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

3. UFES provides the UAV location information to UTM/USS for the relevant UAV. UTM/USS 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

TBD

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

### 6.7.1 Solution overview

This solution address key issues #1.

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 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).

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

NOTE: If the USS/UTM supports Diameter, then UAS authentication can be based on any EAP-based authentication mechanism.

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.

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.

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. 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) which is bound to the UAS ID, UAV-CAA-Level ID, UAV-C ID, Timestamp and a Nonce generated by the USS/UTM. 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. Further the USS/UTM shall generate a UAS root key (KUAS) (e.g. 256-bit) from the long-term credential available as part of UAS subscription information in the USS/UTM to enable UAS security and a KUAS ID shall be generated to uniquely identify a UAS root key in the USS/UTM. The derivation of UAS root Key can be based on the UAS authentication method used and it is out of 3GPP scope. The KUAS ID can be derived by the USS/UTM by generating the hash of the UAS root key and concatenated with the UAS ID. 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 and UAS Security Context (KUAS and KUAS ID).

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, CAA Level UAV ID, UAS ID, KUAS ID, Auth Token and lifetime.

Step 3h. The UFES receives the UAS authentication response message containing CAA Level UAV ID, UAS ID, 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 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 request 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 (KUAS ID, KUAS) similar to the USS/UTM from the long-term credential preconfigured in the UAV. If the locally generated KUAS ID and received KUAS ID matches, then the UAV considers the UAS authentication as successful and locally stores the received CAA Level UAV ID, UAS ID, Auth Token, lifetime, and KUAS ID along with the most recently derived KUAS as part of UAS Security Context. The UAV uses the KUAS ID to uniquely identify the KUAS.

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

Editor’s Note: It is FFS, how the 3GPP system shall enable revocation of UAV or networked UAVC authorisation by the UTM/USS.

Editor’s Note: The need for deriving the key is FFS.

Applicability to EPS:

The UAS Authentication and Authorization procedure shown in Figure 6.7.2-1 and described in this section can be applicable to EPS, with the adaptation of MME instead of AMF, with the HSS/AuC instead of UDM. Further, an EPS authentication is run using EPS AKA as primary condition (instead of primary authentication) before triggering a UAS authentication and authorization. UFES can act as a UAS control function in the 3GPP network.

### 6.7.3 Solution evaluation

TBD

## 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.

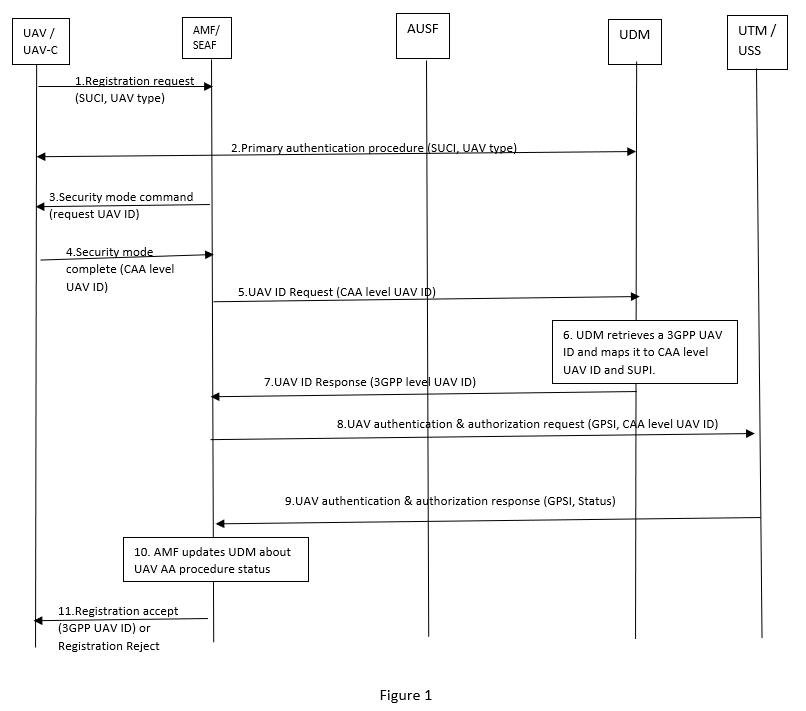


Figure 6.9.2-1: UAS enabled authentication flow

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. 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.

Editor’s Note: The lifetime of the authorisation, e.g. permanent till revocation or one time authorization, is FFS.

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 5: 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.



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 any active C2 connections.

Editor’s Note: Messages used to perform the revocation are FFS.

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

TBD

## 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

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



Figure 6.11.2-1: 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.

Inform PLMN the authorization results with GPSI pair.

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

Editor's note: What identities and credentials (if any) are exchanged with USS/UTM to enable the pairing authorization is FFS

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

Editor's note: How to support revocation of pairing authorization is FFS

### 6.11.3 Solution evaluation

TBC

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

Editor’s Note: This clause will contain the conclusion of the TR

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 |
| 2020-1 | 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 |