|  |
| --- |
| 3GPP TR 33.854 V0.1.0 (2020-08) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® 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.X Solution #X: <Solution name> 17

6.X.1 Solution overview 17

6.X.2 Solution details 17

6.X.3 Solution evaluation 17

7 Conclusions 17

Annex <A>: <Informative annex title for a Technical Report> 18

Annex <X> (informative): Change history 19

# 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)".

# 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, an unauthorized UAVC may take control of UAVs causing tremendous risks to the security of UAS and public safety.

If pairing authorization of UAV and UAVC is not performed securely, an unauthorized UAVC may hijack UAVs causing tremendous risks to the security of UAS and public safety.

The pairing authorization process should be standardized to avoid costly proprietary solutions or potential security risks with respect to proprietary solutions.

If 3GPP system is not capable to receive revocation of 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

The pairing of a UAV and a UAVC shall be authorized by USS/UTM before the 3GPP system can provide UAV and/or UAVC connectivity service used for UAS operations.

3GPP system shall enable UAV and UAVC pairing authentication and authorization by USS/UTM, which provides the outcome to the 3GPP system.

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

Editor’s Note: Whether UAV and UAVC pairing authorization is in scope of this TR is FFS.

## 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.

Besides, 3GPP TS 22.125 [2] gives several security-related requirements of protecting the communication between UAS and UTM/USS, this includes the protection of Remote ID, other exchanged 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) 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 (e.g. 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.X.2-1: UAA procedure**

1. UAV (or UAVC) sends registration request to AMF. It may indicate that this is a registration for UAS.
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.
	1. AMF may optionally request UAS ID from UE.
	2. UAV (or UAVC) responses with UAS ID. It may indicate whether this is a UAV or UAVC.
	3. 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.
	4. USS/UTM response with EAP messages accordingly
	5. EAP messages may continue based on the EAP method used.
	6. …

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

1. Based on the EAP authentication outcome, USS/UTM sends the results to AMF.
2. AMF stores the results, together with SUPI (converted from GPSI), UAS-ID, and UAV/UAVC indicator
3. AMF sends UAS registration complete message to UE

Editor's note:  The UAS Registration IE may be used to determine that UAA is requested, what information in the IE provided by the UE is FFS.

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:  What is provided to the UE following successful UAV authentication and authorization is FFS

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

### 6.1.3 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 |