3GPP TR 22.825 V16.0.0 (2018-09)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Remote Identification of Unmanned Aerial Systems;

Stage 1

(Release 16)

** 

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 Report 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.

Keywords

UAV, UAS, drone, flight, aerial, unmanned

***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.

© 2018, 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](#__RefHeading___Toc523816458)

Introduction [5](#__RefHeading___Toc523816459)

1 Scope [5](#__RefHeading___Toc523816460)

2 References [5](#__RefHeading___Toc523816461)

3 Definitions, symbols and abbreviations [6](#__RefHeading___Toc523816462)

3.1 Definitions [6](#__RefHeading___Toc523816463)

3.2 Abbreviations [6](#__RefHeading___Toc523816464)

4 Overview [6](#__RefHeading___Toc523816465)

5 Use cases [6](#__RefHeading___Toc523816466)

5.1 Use case for Initial authorization to operate [6](#__RefHeading___Toc523816467)

5.1.1 Description [6](#__RefHeading___Toc523816468)

5.1.2 Scenario [7](#__RefHeading___Toc523816469)

5.1.3 Potential service requirements [8](#__RefHeading___Toc523816470)

5.2 Use case for live data acquisition by UTM [8](#__RefHeading___Toc523816471)

5.2.1 Description [8](#__RefHeading___Toc523816472)

5.2.2 Scenario [9](#__RefHeading___Toc523816473)

5.2.3 Potential service requirements [9](#__RefHeading___Toc523816474)

5.3 Use case for data acquisition by law enforcement [10](#__RefHeading___Toc523816475)

5.3.1 Description [10](#__RefHeading___Toc523816476)

5.3.2 Scenario [10](#__RefHeading___Toc523816477)

5.3.3 Potential service requirements [10](#__RefHeading___Toc523816478)

5.4 Use case for enforcement of no-fly zones [10](#__RefHeading___Toc523816479)

5.4.1 Description [10](#__RefHeading___Toc523816480)

5.4.2 Scenario [11](#__RefHeading___Toc523816481)

5.4.3 Potential service requirements [11](#__RefHeading___Toc523816482)

5.5 Use case for distributed close-field separation service [11](#__RefHeading___Toc523816483)

5.5.1 Description [11](#__RefHeading___Toc523816484)

5.5.2 Scenario [12](#__RefHeading___Toc523816485)

5.5.3 Potential service requirements [12](#__RefHeading___Toc523816486)

5.6 Use case for local broadcast of UAS identity [13](#__RefHeading___Toc523816487)

5.6.1 Description [13](#__RefHeading___Toc523816488)

5.6.2 Scenario [13](#__RefHeading___Toc523816489)

5.6.3 Potential service requirements [14](#__RefHeading___Toc523816490)

5.7 Use case of differentiation between UAV specific UE and regular UE attached to UAV [14](#__RefHeading___Toc523816491)

5.7.1 Description [14](#__RefHeading___Toc523816492)

5.7.2 Scenario [14](#__RefHeading___Toc523816493)

5.7.3 Potential service requirements [15](#__RefHeading___Toc523816494)

5.8 Cloud-based NLOS UAV operation [15](#__RefHeading___Toc523816495)

5.8.1 Description [15](#__RefHeading___Toc523816496)

5.8.2 Scenario [16](#__RefHeading___Toc523816497)

5.8.3 Potential requirements [16](#__RefHeading___Toc523816498)

5.9 Use case of UAV fly range restriction [16](#__RefHeading___Toc523816499)

5.9.1 Description [16](#__RefHeading___Toc523816500)

5.9.2 Scenario [17](#__RefHeading___Toc523816501)

5.9.3 Potential service requirements [17](#__RefHeading___Toc523816502)

5.10 Use Case for the UAS Based Remote Inspection [17](#__RefHeading___Toc523816503)

5.10.1 Description [17](#__RefHeading___Toc523816504)

5.10.2 Scenario [18](#__RefHeading___Toc523816505)

5.10.3 Potential service requirements [18](#__RefHeading___Toc523816506)

6 Additional considerations [18](#__RefHeading___Toc523816507)

6.1 Considerations on lawful interception [18](#__RefHeading___Toc523816508)

6.2 Considerations on security [18](#__RefHeading___Toc523816509)

7 Consolidated potential requirements [19](#__RefHeading___Toc523816510)

7.1 General [19](#__RefHeading___Toc523816511)

7.2 Centralised UAV traffic management [20](#__RefHeading___Toc523816512)

7.3 Decentralised UAV traffic management [20](#__RefHeading___Toc523816513)

7.4 Security [21](#__RefHeading___Toc523816514)

8 Conclusions and Recommendations [21](#__RefHeading___Toc523816515)

Annex A: Change history [22](#__RefHeading___Toc523816516)

# 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.

# Introduction

Interest in using cellular connectivity to support Unmanned Aerial Systems (UAS) is strong, and the 3GPP ecosystem offers excellent benefits for UAS operation. Ubiquitous coverage, high reliability and QoS, robust security, and seamless mobility are critical factors to supporting UAS command and control functions. In parallel, regulators are investigating safety and performance standards and Registration and licensing programs to develop a well-functioning private and civil UAS ecosystem which can safely coexist with commercial air traffic, public and private infrastructure, and the general population.

Enabling UAS identification and tracking would allow authorised users (for example air traffic control, public safety agencies) to query the identity and metadata of a UAV and its UAV controller via Unmanned Aerial System Traffic Management (UTM). The UTM stores the data required for UAS(s) to operate. Air traffic control agency uses the UTM server to authorise, enforce, and regulate UAS operation. This would assist in controlling airspace and for public safety applications.

# 1 Scope

The present document identifies the use cases and documents the derived potential requirements for meeting the business, security, and public safety needs for the remote identification and tracking of UAS linked to a 3GPP subscription.

# 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] http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000102131 (Korean only)

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

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

**Unmanned Aerial System**: the combination of a UAV and a UAV controller

**Unmanned Aerial Vehicle**: an aircraft without a human pilot onboard which is remotely controlled

**UAV controller**: a device used to remotely control a UAV

## 3.2 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].

ATC Air Traffic Control

NLOS Non-line-of-sight

UAS Unmanned Aerial System

UAV Unmanned Aerial Vehicle

UCAS Unmanned Aerial Vehicle Collision Avoidance System

UTM Unmanned Aerial Vehicle Traffic Management

# 4 Overview

Ubiquitous coverage, high reliability and QoS, robust security, and seamless mobility are critical factors to supporting UAS functions over cellular networks. In addition, regulators are investigating safety and performance standards and Registration and licensing programs to develop a well-functioning private and civil UAS ecosystem which can safely coexist with commercial air traffic, general aviation, public and private infrastructure, and the general population.

The present document studies the potential use cases and requirements for 3GPP to support remote identification of UAS and the usage of the remote identification.

# 5 Use cases

## 5.1 Use case for Initial authorization to operate

### 5.1.1 Description

As a UAS requests permission to access UAS data services from an MNO, the MNO performs a secondary check (after or in parallel to the initial mutual authentication) to establish the UASs credentials to operate.

The MNO is responsible for transporting and potentially adding additional data to the request to operate from the UAS to an Unmanned Aerial System Traffic Management (UTM). Note that the UTM is a 3GPP entity. This UTM is responsible for the authorization of UAS to operate and checks the credentials of the UAS and UAV operator. One option is that the UTM is operated by air traffic control agencies. It stores all the data regarding the UAV, UAV controller and their live location.

If the UAS fails any part of this check, the MNO may refuse service to the UAS and hence deny permission to operate.

RAN

CN

RAN

CN

RAN

Unmanned Aerial Vehicle Traffic Management (UTM)

UAV controller

UAV

UAS

Figure 5.1.1-1: Initial authorisation to operate

### 5.1.2 Scenario

A UAS is made up of a UAV and a UAV controller which is a physical device used by a UAV operator. One UAV controller may command and control one UAV or a fleet of UAVs. The UAV and the UAV controller both have certain credentials and identities which are factory set, related to the status of the UAS or UAV operator, or related to the operating scenario. This includes unique 3GPP credentials and identities. The communication between the UAV controller and UAV is done via 3GPP communication service offered by MNO.

Detection of UAS communication is possible in an MNO network and if UE subscription does not allow such communication it is rejected.

Permission for a UE to function as an aerial UE in the 3GPP network can be identified via subscription information. The network may use this information to perform the necessary control and apply relevant functions. Based on this subscription information uplink power adjustment and frequency band alteration can be applied in order UAS communication not to have impact on other types of communication. In addition to UAS subscription information UE can indicate a radio capability to the network which may be used to identify a UE with relevant functions for UAS communication in a 3GPP network.

In this scenario, the UAS has been switched on in order for the UAV operator to fly the UAV using the UAV controller. The UAV operator pairs the UAV and the UAV controller for UAS operation through some mechanism.

The UAV passes UAV data to onboard 3GPP UE. The UE authenticates with MNO. In parallel to the attach request, the UE sends the UAV data & 3GPP identifiers to the Unmanned Aerial System Traffic Management (UTM), requesting initial permission to attach to the network to fly and using certain services provided by UTM. Subject to national regulatory UTM requirements, a UAS may need to go through several authentication and authorization processes before a UAS can be fully operated, e.g. after finishing the initial authentication for establish connection with the UTM, a UAV may need to go through additional application level authentication to activate some UTM services, such as flight monitoring or collision avoidance service. Therefore, a UAS may need to provide different UAS identity data according to the level of the authorization and authentication process required by the UAS.

If the request towards UTM is coming from UE without subscription information for drone communication, then the request shall be rejected.

The same operation is done by the UAV controller using its own credentials and identifiers.

During the initial authorization procedures, the MNO and UTM need to be able to associate the UAV and the UAV controller as a UAS.

If the UTM rejects a request for some reasons, e.g. incorrect identities or credentials, or UAS element(s) are operating in the area which is prohibited, the MNO rejects the attach request of the UAV and/or UAV controller of the UAS.

If both registration requests are accepted for the UAS, the UAV operator can use the UAV controller to fly the UAV by transmitting commands from the UAV controller to the UAV via 3GPP network.

### 5.1.3 Potential service requirements

The 3GPP system shall enable a UAS to send the following UAV data to a UTM: unique identity (this may be unique 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 and time, mission type, route data, operating status.

The 3GPP system shall enable a UAS to send the following UAV controller data to a UTM: unique identity, UE capability of the UAV controller, position, owner identity, owner address, owner contact details, owner certification, the identity of the UAV operator who operate the UAV controller, UAV operator license and certification.

The 3GPP system shall enable a UAS to send different UAS data to UTM based on the different authentication and authorizations level which are applied to the UAS.

The 3GPP system shall support capability to extend UAS data being sent to UTM with the evolution of UTM and its support applications in future.

The 3GPP system shall protect against spoofing attacks of the UAS identities.

The 3GPP system shall protect the integrity of the message(s) sent from UAS to a UTM containing the UAS identities.

The 3GPP system shall enable a UE in a UAS to send the following identifiers to a UTM: IMSI, IMEI, MSISDN.

The 3GPP system shall protect the confidentiality of the message(s) sent between UAS to a UTM containing the UAS identities.

The 3GPP system may enable an MNO to augment the data sent to a UTM with the following: network-based positioning information, preconfigured pairing data.

A UAS may optimise subsequent messages sent to an UTM by omitting unchanged static or semi-static data (e.g. owner identity, owner address, owner contact details, owner certification).

The UTM shall be able to associate the UAV and UAV controller, identify them as a UAS, and authorise a UAS to operate.

The UTM shall be able to coordinate the route data provided in the authorisation to operate and change it if needed.

The UTM shall be able to refuse authorisation for a UAS to operate.

The UTM shall be able to inform an MNO of the outcome of an authorisation to operate.

An MNO shall be able to enforce the authorisation for a UAS to operate (e.g. by enabling or disabling communication between the UAV and UAV controller).

The 3GPP system shall enable an MNO to allow a UAS authorisation request only if appropriate subscription information is present.

## 5.2 Use case for live data acquisition by UTM

### 5.2.1 Description

Infrastructure may be deployed in certain regions to ensure the safety of UAS operations. The purpose of such an infrastructure would be to keep drones separated from each other and also from the few aircraft such as low flying helicopters with which they may need to share the airspace.

The UTM may offer an Unmanned Aerial Vehicle Collision Avoidance System (UCAS) service. The primary scope of the 3GPP involvement in such a UCAS would be to provide accurate live positioning information into the UTM from the UAS or MNO, thereby offering a primary or complementary positioning solution able to allow an independent verification of the location reported by the UCAS, if applicable, and to ensure timely feedback from the UTM to the UAS.

Most drones of a certain class already have collision avoidance systems on board. Such systems range is very wide from very poor to good – depending on size, quality, price of the drone and the know-how of the manufacturer. Active control from UTM is important and onboard systems can be used as a backup.



Figure 5.2.1-1: Live data acquisition by UTM

### 5.2.2 Scenario

Several UAVs are making deliveries to an office block simultaneously. They are each registered with the UTM. Each UAS is transmitting accurate positional information, which may be supplemented by the service MNO, to the UTM. The UTM has agreed their route data with the authorization to operate. The UTM offers a UCAS service.

The UAS provides the UTM with its live location.

The UTM may receive location information related to manned air traffic. When the UTM detects that there is a danger of loss of separation between a UAS under its control and a manned aircraft the UTM may issue a course change commend to the appropriate UAS.

As the UTM notices that the multiple UAVs pass some metric of proximity defined by speed of aircraft, density of airspace, etc. and decided to intervene to help prevent any collision. The UTM sends a notification message towards UAV controller to warn for possible collision. If after notification message there is no change of behaviour of UAV the UTM may send route change data to the UAS.

The route modifications are transmitted to each UAS and are incorporated into the planned routes of each UAS.

### 5.2.3 Potential service requirements

The 3GPP system shall enable a UTM to be aware of the identity/identities of a UAS.

The 3GPP system shall enable a UAS to update a UTM with the live location of a UAV.

The 3GPP system shall enable a UAS to send the location of the UAV and UAV controller towards UTM with at least a periodicity of 1 update per second.

The 3GPP system may enable an MNO to supplement location information sent to a UTM.

NOTE: this supplement may be trust-based (i.e. the MNO informs the UTM that the UAV position information is trusted) or it may be additional location information based on network information.

The 3GPP system shall enable a UTM to send route modification information to a UAS with a latency of less than 1 second.

## 5.3 Use case for data acquisition by law enforcement

### 5.3.1 Description

Police respond to a nuisance complaint about a UAV. Before entering the area where the report was made, they query the various sources of information about what UAS are operating in the area to identify and gather information about any operating UAV in that area.



Figure 5.3.1-1: Data acquisition by law enforcement

### 5.3.2 Scenario

Police respond to a nuisance complaint about a UAV. Before entering the area where the report was made, they query the UTM to see if any have a live UAV in the area. For example, the police might supply a civic address, geographic polygon, a list of identities of known persistent offenders, etc. The UTM would return the subscription, equipment identity, route data, live location, and all data for the flight of any devices operating as a UAS in the submitted area or matching the submitted identity.

This could lead to a further request for more data to attempt to make visual contact with (a) the UAV, and (b) the UAV operator.

### 5.3.3 Potential service requirements

The 3GPP system shall enable an authorised official to query a UTM for information and identities of an active UAS when an authorised official provides a subset of UAS data (e.g. an IMSI, general location, or IMEI).

The 3GPP system shall enable an authorised official to query a UTM for the current location(s) of an active UAS when an authorised official provides a subset of UAS data (e.g. an IMSI, general location, or IMEI).

The 3GPP system shall enable a UTM to authenticate the identity and authority of the official making a request for UAS identity and information.

## 5.4 Use case for enforcement of no-fly zones

### 5.4.1 Description

Some sort of infrastructure may be deployed in certain regions to ensure the safety of UAS operations outside of the airspace open to civil aviation. The purpose of such an infrastructure would be to provide control methods for enforcing flight restrictions on UAVs. Such an Unmanned Aerial System Traffic Management (UTM) server would require the ability to identify, locate, and instruct the UAS (via the UAV controller).

The primary scope of the 3GPP involvement in such an Unmanned Aerial Vehicle Collision Avoidance System (UCAS) would be to provide accurate live positioning information into the UTM from the UAS or MNO, and to ensure timely feedback from the UTM to the UAS (via the UAV controller).



Figure 5.4.1-1: Enforcement of no-fly zones

### 5.4.2 Scenario

A UAS is approaching the no-fly zone around an airport. Other no-fly zones may be around prisons, highway roads, hospitals, road or crime incidents. The initial authorisation to fly did not contain a route which included this path as the UAV is small enough to not require a route in advance to be granted permission to operate. Or the no-fly zone was temporarily created because of a particular incident.

The UAS is transmitting accurate positional information, which may be supplemented by the serving MNO, to the UTM.

As the UTM notices that the UAV approaches the edge of the no-fly zone, the UTM decides to send warning to the UAV operator (via the UAV controller) with the details of the no-fly zone. If UAV has reached the edge of the no-fly zone the UTM decides to intervene to prevent any further incursion. The UTM determines a route to remove the UAV from the no-fly zone and provides a route modification to the UAS to achieve this correction. Optionally, the details of the no-fly zone are sent to the UAV controller for user information.

The route modifications are transmitted to the UAS and are executed by the UAS to correct the position of the UAV.

### 5.4.3 Potential service requirements

The 3GPP system shall enable a UAS to update a UTM with the live location of a UAV.

The 3GPP system may enable an MNO to supplement location information sent to a UTM.

The 3GPP system shall enable a UTM to send route modification information to a UAS with a latency of less than [500ms].

The 3GPP system shall enable a UTM to send a notification to a UAV controller with a latency of less than [500ms].

## 5.5 Use case for distributed close-field separation service

### 5.5.1 Description

There is a requirement to provide separation between UAVs. A collision incident can cause property damage, interference to a UAS’s objectives, and may pose a safety threat. Therefore, regardless of network conditions, a service to ensure separation between UAVs is desirable.

When in visual line-of-sight to the UAV operator, separation can be provided manually through command & control mechanisms. The UAV operator is responsible to maintain well-clear separation from other aircraft, buildings, and other obstacles.

When beyond visual line-of-sight, the UAV operator may be offered video or instrumental feedback to manually maintain separation. In addition, a UTM may offer a separation service as documented in clause 5.2 of the present document.

When out of coverage and out of visual line-of-sight, there can be no manual input and there can be no UTM-offered separation service. In this scenario, a distributed separation service is desirable.

### 5.5.2 Scenario

A UAS is operating a mission in San Diego to transport blood for transplant surgery between 2 hospitals. The UAVs are flow under waypoint guidance and operate with a high degree of automation in normal operating modes.

Because of the geography of San Diego, much of the route is planned to fly over canyons due to the direct route and the lower population density providing a lower risk factor. The canyons often have poor radio coverage due to physical distance from, and obstruction of, the nearest radio towers.

These canyons also act as “highways” for UAVs due to the geography and risk factors. Therefore, UAV density is often quite high. Also, to take into account is the requirement to route around the U.S. Marine Corps base at Miramar which also provides a concentration of UAVs at the boundary of the no-fly zone.

In this scenario a faster moving drone is approaching behind the subject of this use case. As there is limited radio coverage, both UAVs are in an automated mode of operation and there is no connection to a UTM to provide a separation service. They require distributed intelligence to maintain separation or else a collision will occur.

Both UAVs are fitted with 3GPP ProSe-enabled communication modules and discover each other at a safe distance. They negotiate a separation method (typically they separate in the vertical plane) and execute route modifications to adapt to the presence of the other. This procedure also takes into account the presence of other UAVs in the area.

The UAVs pass each other safely and resume their previously planned route.

### 5.5.3 Potential service requirements

Editor’s note: These potential requirements require cross-checking with regulators and UAS OEMs before inclusion into normative work.

The 3GPP system shall enable a UAV to broadcast the following identity data in a short-range area for collision avoidance: [UAV type, current location and time, route data, operating status].

The 3GPP system shall enable UAV to broadcast the identity information which preserves the privacy of the owner of the UAV and the UAV operator.

The 3GPP system shall enable a UAV to receive local broadcast communication transport service from other UAV in short range.

A UAV shall be able to use a direct UAV to UAV local broadcast communication transport service when served or not served by a 3GPP network.

A UAV shall be able to use a direct UAV to UAV local broadcast communication transport service when served or not served by the same 3GPP network.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service at relative speeds of up to 320 kmph.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service at absolute speeds of up to 160 kmph.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service with variable message payloads of 50-1500 bytes, not including security-related message component(s).

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can maintain a separation distance between two UAVs of greater than 50 m.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which supports a range of up to 600 m

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which supports a range sufficient to give the UAVs ample time to perform manoeuvres to maintain a separation distance of 50m (e.g. 6.5 seconds).

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can transmit messages at a frequency of at least 10 messages per second.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can transmit messages with an end-to-end latency of at most 100 ms.

## 5.6 Use case for local broadcast of UAS identity

### 5.6.1 Description

According to clause 5.3 of the present document, airspace administration shall be able to query the UTM for identity, location, and associated information about a UAS. However, local broadcast of a UAS identity provides a backup means of ID and tracking if the network is compromised, degraded, or unavailable. If UAS were to locally broadcast their identity and other information, this would allow airspace enforcement or other authorized personnel with the appropriate equipment to discover UAS within proximity.



Figure 5.6.1-1: Data acquisition by law enforcement

### 5.6.2 Scenario

Police respond to a nuisance complaint about a UAV. Network coverage is not good in this area, and so before attempting to query the UTM to see if any have a live UAV in the area the police responding to the report in the local area uses handheld equipment to scan for any UAS broadcasting their identities in the local area.

Once such a UAS is found, the police may use the received ID to query the UTM for more information, or the police may use information in the ID message itself to trace the source of the messages (either a UAV of a UAV controller).

This could lead to a further request for more data to attempt to make visual contact with (a) the UAV, and (b) the UAV operator.

### 5.6.3 Potential service requirements

Editor’s note: These potential requirements require cross-checking with regulators and UAS OEMs before inclusion into normative work.

The UAS shall be able to locally broadcast its identity and location.

NOTE: the locally broadcast information should not expose personally identifiable information to general users.

The UAS shall be able to locally broadcast its identity via local broadcast with a rate of at least once per 1s.

The UAS shall be able to locally broadcast its identity up to a range of 500m.

## 5.7 Use case of differentiation between UAV specific UE and regular UE attached to UAV

### 5.7.1 Description

From the MNO’s point of view, an MNO may want to differentiate the UE which is specific for UAS use (UAS-capable) with the regular ground based UEs, as well as to identify the different class of UAV (e.g. small/big UAVs) for the following reasons:

(1) To provide better service to the UAVs. As we know, airborne UAV may receive more DL signal interference from more RANs because UAVs can see more cells/RANs in the air (described in TR 36.777). If airborne status can be identified, MNO can use differentiated/optimized power control methods. Moreover, if UAV’s type can be identified, an MNO can translate the UAV class to mobility parameters (e.g. Time to Trigger used for handover), which can be used for mobility enhancements.

(2) To protect the network. The airborne UAV may produce higher UL signal interference to the UEs on the ground (Described in TR 36.777), if the UAS-capable UE can be identified, suitable mechanisms or procedures can be used to migrate interference.

(3) To differentiate charging rules. MNOs may want to charge different subscription fees for airborne UAV with UAS-capable UE vs. regular UEs.

Also from the regulatory point of view, only certain type of UAV with certain 3GPP communication capabilities may be allowed to be operated in certain areas, and the MNOs may have the responsibility to identify the unauthorized airborne UAV that may because that type or communication capability of UAV is not allowed (e.g. UAV attached with a regular cell phone) in that area, and report to UTM or law enforcement.

Some UAS may seek to operate without initial authorization from the UTM. In addition, they may attempt to avoid detection from the 3GPP system and being identified as UAS-capable UE. For instance, they may embed a terrestrial 3GPP UE and identify as a regular 3GPP UE.

These UAS may hinder network performance and represent a breach of regulation in some airspaces. However, even in the absence of an explicit identification as a UAS-capable UE, the 3GPP system may detect, based on implicit information such as mobility pattern history and other RAN airborne UE detection mechanism, that the 3GPP UE is actually a UAS-capable UE in flying mode. In that case, an MNO may notify the UTM that a specific UE is believed to be in flying mode, to provide live positioning information into the UTM

### 5.7.2 Scenario

During initial authorisation operate procedures, MNO will identify whether this UAV is UAS-capable UE with certain 3GPP UAS communication capability, and interaction capability with UTM, or the UAV is attached external UE (e.g. a smart phone) with limited or no 3GPP UAS communication capability as well as interaction capability with UTM. If the UAV is authorized to be airborne, MNO may base on the type of the UE (UAS specific UE vs. regular UE) to schedule network resource accordingly, such as use different /optimized power control methods and mobility enhancement procedures, more specifically, mobility parameters for this UAV according to the type (e.g. the speed limit reflected by the type can affect the parameters used for handover). If the UAV is embedded with UAS-capable UE, which means the UAV can interact with UTM, so MNO may establish further communication between UAS and UTM. In addition, different charging rules will be used to the UAV by the serving MNO.

Also an MNO may retrieve those capability/type of UAV according to subscription identifiers information, so MNO can determine whether or not to allow the UE to use certain Aerial UE function (defined in TS 36.300) or enable certain RAN capability which can be used for mobility enhancement and interference mitigation.

If this UAV is embedded with a UAS-capable UE but pretend to be a regular ground base UE. It may pass MNO’s authentication and become airborne. Later MNO may identify that this is a rogue UAV basing on its moving behaviours which is not matched with its subscription used for the authentication. The MNO will report this unauthorized UAV with related information to the UTM or law enforcement. MNO may also report an unauthorized UAV which only equips with ground based UE but fly into an area which only UAV with UAS-capable UE is allowed.

### 5.7.3 Potential service requirements

The 3GPP system shall provide the capability for an MNO to receive the UAS information regarding its 3GPP communication capabilities.

The 3GPP system shall support the UAS identification data which can differentiate the UAS with UAS-capable UE and the UAS with non-UAS-capable UE.

NOTE: UAS-capable UE refers to the UE which support interaction capability with UTM and certain 3GPP communication features which 3GPP provides for UAS.

The 3GPP system shall support identification and reporting unauthorized UAVs to a UTM.

## 5.8 Cloud-based NLOS UAV operation

### 5.8.1 Description

In most countries, the operation of UAV is limited to the line-of-sight control i.e., the operation of UAV is allowed only when human UAV operators can directly see the UAV. Also, most countries prohibit operation of UAV at night.

Recently, Korean government launched a special program which allows UAV operation even when a UAV operator is not in line-of-sight of a UAV or when the UAV operates at night. [2]

But, to apply for this special program, there are certain conditions. For example:

- UAV is equipped with lights for collision-avoidance purpose. These lights should be visible up to 5 KM away.

- UAV is equipped with support for auto-pilot functionality, more than one way of communication channel (e.g. RF + LTE).

- Observers who can monitor a UAV should be dispatched, if a UAV operator controls the UAV out of line-of-sight.

These conditions will evolve or be relaxed in the future, as alternative approaches and technologies are available or enough tests have been performed to prove safety of NLOS UAV operation. For example:

- Observers can be replaced to non-human system which can detect or monitor UAVs.

- Light used for collision-avoidance can be replaced to other communication-based method. (e.g. broadcast of identifiers using direct 3GPP communication)

- Back-up communication path can be provided even within 3GPP systems. (e.g. using direct/indirect 3GPP communication simultaneously)



Figure 5.8.1-1: Identification of NLOS UAV

### 5.8.2 Scenario

A UAV control center operates a UAV using 3GPP communication. Through this 3GPP communication link toward the UAV, the UAV control center can see the video image transmitted by the UAV and sends flight command to the UAV.

To avoid collision among UAVs, the UAV transmits identification messages to identify itself to other UAVs, using direct device connection. These identification messages can be received also by observation devices deployed by UAV service operator on the ground. These ground-based observation devices report the location and the identity of the detected UAVs to the UAV control center, to assist the control of the UAV. Furthermore, national ATC system can be enhanced to receive identification messages transmitted by UAVs using 3GPP communication, to have a nation-wide view of aerospace.

### 5.8.3 Potential requirements

The 3GPP system shall be able to support a UAV to transmit a message to identity the UAV via direct device connection.

The 3GPP system shall be able to support direct device connection between UAVs to transmit messages to identity the UAVs.

Editor’s note: It is FFS up to which distance the direct device connection needs to support

The 3GPP system shall be able to support a UAV to transmit a message to identity the UAV via direct device connection in addition to network connection.

## 5.9 Use case of UAV fly range restriction

### 5.9.1 Description

Considering beyond visual line-of-sight remote controlled UAV using cellular technologies can expose some public safety and security concerns in some countries, therefore there is a need to consider the case which needs to apply restriction on the fly range of a remote controlled UAV, such as to prevent out-of-sight flying, restriction on the distance range between the UAV and the UAV controller, or the geographic range of UAV can fly.

In addition, because of the roaming consideration, preventing controlled UAV crossing different PLMNs may also be required.

Therefore, to address those public security and charging issues, we should define and limit the fly range of the UAV, such as controlling range between UAV and UAV controller.

### 5.9.2 Scenario

A UAV, remotely controlled by a UAV controller, both of which are connected through cellular network, is flying away from the UAV controller beyond certain range limit which is based on the type, subscription information, or characteristic of the UAV. The UAV and the UAV controller are transmitting their accurate positional information, which may be supplemented by the serving MNO, to the UTM.

The UTM notices that the UAV is flying over the range from the UAV controller basing on the information from UAV and UAV controller, as well as may come from network, the UTM decides to send a warning to the UAS operator (via the UAV controller). If UAV has reached certain threshold, the UTM may decide to intervene to force the UAV to fly closer back to the UAV controller or fly back to the area which it is allowed to fly in. If the UAV flies into different roaming area, different or additional charging rule may be applied by the MNO.

### 5.9.3 Potential service requirements

The 3GPP system shall enable a UAS to update a UTM with the live location information of a UAV and its UAV controller.

The 3GPP system shall be able to supplement location information of UAV and its UAV controller.

The 3GPP system shall support a UTM to consume Location Service provided by the network.

The 3GPP system shall be able to enforce the authorisation for an in-flight UAS to operate basing on UAS subscription information or under the instructions from UTM (e.g. by enabling dedicated control channel between UAS and UTM, or enabling or disabling communication between the UAV and UAV controller).

## 5.10 Use Case for the UAS Based Remote Inspection

### 5.10.1 Description

The UAS has been broadly used for providing remote inspection services, e.g. inspection of buildings, assents, properties, power line infrastructure, forest, agricultural fields, or disaster scenes, etc. Such services would requirea longer flying distance and reliable connection between the UAV and the UAV controller. Therefore, to enable UAS based remote inspection service using 3GPP connectivity, the 3GPP network shall be able to assist UAS operation with the following characteristics:

- The 3GPP network shall be able to support low latency transmission for delivering commands sent by the UAV controller and response message sent by the UAV controller and UAV, respectively.

- Bi-directional high throughput from the UAV to the UAV controller via 3GPP network, e.g. to send real-time video.

Also for the UAS, the UAV and UAV controller needs to support

- network assisted UAS discovery to be identified and operate as a UAS

- 3GPP UE capabilities

When a UAS has been identified and granted permission for operation after successful UAS discovery, the MNO provides UAS services such that the UAV operator can use the UAV controller to fly the UAV via the 3GPP network. The 3GPP network needs to able to provide low latency, and high reliability connection for transporting UAV commands/response between the UAV controller and the UAV. Depending on the UE capability and use cases, bi-directional high throughput may be needed for the data session to allow the UAV for providing real-time remote video to the UAV controller.

The MNO is responsible for transporting and potentially adding additional data to the command of the UAV controller to operate the UAV.

If the UAS is detected by the MNO/UTM for some misbehaviors, the MNO/UTM can take over the UAV controller and send the UAV command directly to fly the UAV.



Figure 5.10.1-1: Network assisted UAS Operation (No direct communication between the UAV controller and the UAV)

### 5.10.2 Scenario

The UAV controller and UAV have been switched on to serve remote inspection mission for power line infrastructure. The MNO initiates network assisted UAS discovery procedure.

After successful Network assisted UAS discovery, the UTM can then start to track the UAS and the 3GPP network enables the 3GPP connectivity to assist the UAS operation.

The UAV controller requests the 3GPP network to establish a data connection which can provide low latency and reliable connectivity for transporting UAV commands and receiving UAV responses.

The 3GPP network establishes a route via control plane path or data plane for the UAV and the UAV controller, which can be anchored in the same RAN node, routed between two different RAN nodes that serve UAV and UAV controller, respectively, control plane or user plane gateway function, or a local DN at the edge.

The UAV starts to record the real-time video and transport it to the UAV controller using the 3GPP connectivity via 3GPP network.

### 5.10.3 Potential service requirements

An MNO shall be able to enforce the authorisation for assisting a UAS to operate, e.g. by establishing a reliable route within 3GPP network to deliver the commands/control messages between the UAV and UAV controller.

The 3GPP network shall be able to support roaming when providing network assisted UAS operation.

# 6 Additional considerations

## 6.1 Considerations on lawful interception

It shall be possible to support lawful interception for UAS traffic.

## 6.2 Considerations on security

The 3GPP system shall support confidentiality protection of identities related to the UAS and personally identifiable information.

The 3GPP system shall support the capability to provide different levels of integrity and privacy protection for the different connections between UAS and UTM as well as the data being transferred via those connections.

The 3GPP system shall support non-repudiation of data sent from the UAS to UTM.

Data held at the UTM may be subject to local data retention and privacy regulations.

# 7 Consolidated potential requirements

## 7.1 General

The UTM shall be able to associate the UAV and UAV controller, identify them as a UAS, and authorise a UAS to operate.

The UTM shall be able to refuse authorisation for a UAS to operate.

The 3GPP system shall enable a UAS to send the following UAV data to a UTM: unique identity (this may be unique 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.

The 3GPP system shall enable a UAS to send the following UAV controller data to a UTM: unique identity, UE capability of the UAV controller, position, owner identity, owner address, owner contact details, owner certification, the identity of the UAV operator who operate the UAV controller, UAV operator license and certification.

The 3GPP system shall enable a UAS to send different UAS data to UTM based on the different authentication and authorizations level which are applied to the UAS.

The 3GPP system shall support capability to extend UAS data being sent to UTM with the evolution of UTM and its support applications in future.

The 3GPP system shall enable a UE in a UAS to send the following identifiers to a UTM: IMSI, IMEI, MSISDN.

The 3GPP system may enable an MNO to augment the data sent to a UTM with the following: network-based positioning information, preconfigured pairing data.

NOTE: this augmentation may be trust-based (i.e. the MNO informs the UTM that the UAV position information is trusted) or it may be additional location information based on network information.

A UAS may optimise subsequent messages sent to an UTM by omitting unchanged static or semi-static data (e.g. owner identity, owner address, owner contact details, owner certification).

The UTM shall be able to inform an MNO of the outcome of an authorisation to operate.

The 3GPP system shall enable an MNO to allow a UAS authorisation request only if appropriate subscription information is present.

An MNO shall be able to enforce the authorisation for a UAS to operate (e.g. by enabling or disabling communication between the UAV and UAV controller).

The 3GPP system shall enable a UTM to be aware of the identity/identities of a UAS.

The 3GPP system shall enable a UAS to update a UTM with the live location information of a UAV and its UAV controller.

The 3GPP system may enable an MNO to supplement location information sent to a UTM.

NOTE: this supplement may be trust-based (i.e. the MNO informs the UTM that the UAV position information is trusted) or it may be additional location information based on network information.

The 3GPP system shall support a UTM to consume Location Service provided by the network.

The 3GPP system shall enable a UAS to send the location of the UAV and UAV controller towards UTM with at least a periodicity of 1 update per second.

The 3GPP system shall enable an authorised official to query a UTM for information, location, and identities of an active UAS when an authorised official provides a subset of UAS data (e.g. an IMSI, general location, or IMEI).

An MNO shall be able to enforce the authorisation for assisting a UAS to operate, e.g. by establishing a reliable route within 3GPP network to deliver the commands/control messages between the UAV and UAV controller.

The 3GPP network shall be able to support roaming when providing network assisted UAS operation.

The 3GPP system shall provide the capability for an MNO to receive the UAS information regarding its 3GPP communication capabilities.

The 3GPP system shall support the UAS identification data which can differentiate the UAS with UAS-capable UE and the UAS with non-UAS-capable UE.

NOTE: UAS-capable UE refers to the UE which support interaction capability with UTM and certain 3GPP communication features which 3GPP provides for UAS.

The 3GPP system shall support identification and reporting unauthorized UAVs to a UTM.

## 7.2 Centralised UAV traffic management

The UTM shall be able to coordinate the route data provided in the authorisation to operate and change it if needed.

The 3GPP system shall enable a UTM to send route modification information to a UAS with a latency of less than [500ms].

The 3GPP system shall enable a UTM to send a notification to a UAV controller with a latency of less than [500ms].

The 3GPP system shall be able to enforce the authorisation for an in-flight UAS to operate basing on UAS subscription information or under the instructions from UTM (e.g. by enabling dedicated control channel between UAS and UTM or by enabling or disabling communication between the UAV and UAV controller).

## 7.3 Decentralised UAV traffic management

The 3GPP system shall enable a UAV to broadcast the following identity data in a short-range area for collision avoidance: [UAV type, current location and time, route data, operating status].

The 3GPP system shall enable UAV to broadcast the identity information which preserves the privacy of the owner of the UAV and the UAV operator.

The 3GPP system shall enable a UAV to receive local broadcast communication transport service from other UAV in short range.

A UAV shall be able to use a direct UAV to UAV local broadcast communication transport service when served or not served by a 3GPP network.

A UAV shall be able to use a direct UAV to UAV local broadcast communication transport service when served or not served by the same 3GPP network.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service at relative speeds of up to 320kmph.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service at absolute speeds of up to 160kmph.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service with variable message payloads of 50-1500 bytes, not including security-related message component(s).

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can maintain a separation distance between two UAVs of greater than 50m.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which supports a range of up to 600m

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which supports a range sufficient to give the UAVs ample time to perform manoeuvres to maintain a separation distance of 50m (e.g. 6.5 seconds).

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can transmit messages at a frequency of at least 10 messages per second.

The 3GPP system shall support a direct UAV to UAV local broadcast communication transport service which can transmit messages with an end-to-end latency of at most 100ms.

The 3GPP system shall be able to support direct device connection between UAVs to transmit messages to identity the UAVs.

Editor’s note: It is FFS up to which distance the direct device connection needs to support

The 3GPP system shall be able to support a UAV to transmit a message to identity the UAV via direct device connection in addition to network connection.

The UAS shall be able to locally broadcast its identity and location.

NOTE: the locally broadcast information should not expose personally identifiable information to general users.

The UAS shall be able to locally broadcast its identity via local broadcast with a rate of at least once per 1s.

The UAS shall be able to locally broadcast its identity up to a range of 500m.

## 7.4 Security

The 3GPP system shall protect against spoofing attacks of the UAS identities.

The 3GPP system shall protect the integrity of the message(s) sent from UAS to a UTM containing the UAS identities.

The 3GPP system shall protect the confidentiality of the message(s) sent between UAS to a UTM containing the UAS identities.

The 3GPP system shall support non-repudiation of data sent from the UAS to UTM.

The 3GPP system shall support the capability to provide different levels of integrity and privacy protection for the different connections between UAS and UTM as well as the data being transferred via those connections.

The 3GPP system shall support confidentiality protection of identities related to the UAS and personally identifiable information.

The 3GPP system shall enable a UTM to authenticate the identity and authority of the official making a request for UAS identity and information.

Data held at the UTM may be subject to local data retention and privacy regulations.

It shall be possible to support lawful interception for UAS traffic.

# 8 Conclusions and Recommendations

The present document contains consolidated potential requirements for the support of remote identification and the services based on remote identification of UAS over cellular connection.

The present document recommends that 3GPP should create normative service requirements based on the consolidated potential requirements identified in this study in order to better serve the UAS ecosystem with cellular connectivity.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 24/08/2018 | SA1#83 | S1-182502 |  |  |  | FS\_ID\_UAS: overview | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182504 |  |  |  | ID\_UAS – enhancement on initial UAV authorization operation | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182505 |  |  |  | ID\_UAS – enhancement on use case for initial authorization to operate | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182506 |  |  |  | FS\_ID\_UAS: Update Definition and Use case 5.1 | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182091 |  |  |  | Comment on the use case 5.2 for live data acquisition by UTM | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182728 |  |  |  | FS\_ID\_UAS: potential requirements for live data acquisition by UTM | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182729 |  |  |  | FS\_ID\_UAS: use case for distributed close-field separation service | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182730 |  |  |  | FS\_ID\_UAS: use case for local broadcast of UAS identity | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182732 |  |  |  | New use case for detection and management of a rogue UAS | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182537 |  |  |  | Cloud-based NLOS UAV operation | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182733 |  |  |  | ID\_UAS – Use case of UAV fly range restriction | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182538 |  |  |  | FS\_ID\_UAS: Use case of UAS Based Remote Inspection | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182539 |  |  |  | ID\_UAS – additional consideration for security | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182540 |  |  |  | FS\_ID\_UAS: consolidated potential requirements | 0.1.0 |
| 24/08/2018 | SA1#83 | S1-182541 |  |  |  | FS\_ID\_UAS: conclusion and recommendation | 0.1.0 |
| 2018-09 | SA#81 | SP-180781 |  |  |  | Raised to v.1.0.0 for presentation to SA | 1.0.0 |
| 2018-09 | SA#81 | SP-180781 |  |  |  | Raised to v.16.0.0 following one-step-approval by SA#81 | 16.0.0 |