Leveraging 3GPP Cellular Network Mechanisms to support UAS operations

March 2022

Table of Contents

Leveraging 3GPP Cellular Network Mechanisms to support UAS operations 1

1.Scope, References, Terminology 4

1.1 Scope 4

1.2 References 5

1.3 Terminology and Abbreviations 6

2. Background on UAS Regulatory Requirements for Remote Identification and Lawful Intercept 7

2.1 Remote Identification 7

2.2 FAA Remote Identification 10

2.2.1 Overview.....10

2.2.2 UAS Serial Number.....11

2.2.3 Spectrum 11

2.2.4 Remote Identification Message Elements 11

2.2.5 Performance requirements:.....12

2.2.6 Applicability of Remote ID and Tracking Requirements.....13

2.2.7 Remote ID USS for Networked Remote ID.....14

2.3 EASA Remote Identification 14

2.4 Networked Remote ID 15

2.5 Lawful Interception (LI) 15

3. Clarification of Scope 16

3.1 3rd Generation Partnership Program (3GPP) 16

3.2 USS provider 17

4. Overall Architecture for UAS Enablement via 3GPP Systems 18

4.1 ACJA Reference Architecture 18

4.1.1 Identification of Roles.....18

4.1.2 Overall Architecture and Assumptions 21

5. Enabling Remote Identification Via 3GPP Technologies 32

5.1 Enabling Networked Remote Identification 32

5.2 Enabling Broadcast Remote Identification 32

5.2.1 Technologies currently referred to in ASTM F38 and ASD-STAN standards 32

5.2.2 Using 3GPP Radio Links.....32

6. Use of Cellular Connection for Remote ID and C2.....34

6.1 Scenarios for Cellular Connectivity 34

6.2 Cellular Connectivity for C2, UAV-USS Communications, and Networked Remote ID 35
7. Location and Flight Tracking 36
8. Security Aspects 37
8.1 Overall security architecture of the UAS-USS model 37
8.2 Security model for UAS authentication/authorization to USS via the 3GPP MNO 37
8.3 C2 privacy and integrity 38
8.4 Remote Identification Security 38
8.4.1 Objectives of Security Model for Remote Identification 38
8.4.2 Prerequisites to 1609.2-Secured UAS ID & Tracking 39
8.4.3 Relationship Between UAS Identity, Certificate and 1609.2 Authentication 40
8.4.4 Certificate Management Services 40
8.4.5 Networked RID privacy and integrity 44
8.4.6 Broadcast RID privacy and integrity 44
9. Appendix: 3GPP System Architecture 46
9.1 EPS System Architecture 46
9.2 5GS System Architecture 47
9.3 Registration and Connectivity Services 48
9.4 Exposure of Network Functions 49
9.5 Location Services 52
About the GSMA 55
About the GUTMA 55

1.Scope, References, Terminology

1.1 Scope

This document focuses on analyzing how cellular networks and related services can be leveraged to support UAS operations (including Networked Remote ID, UAV connectivity for command and control, location and flight tracking, and security), including how they support ASTM 3411-19 Standard Specification for Remote ID and Tracking and future versions. This include an analysis of how additional broadcast mechanisms can be supported in a future revision of F3411.

This document leverages the 3GPP architecture and mechanisms defined in 3GPP Release 17 for UAS, providing a reference to how they can be used but without mandating the use of any of such mechanisms. It assumes a high reliance by the mobile network operators on the USS for UAV authentication and authorization, and for policing of UAV communications via the cellular infrastructure.

As per the Work Task #1 Terms of Reference, this deliverable contains technical views and contributions meant as input to the 3GPP work, to ASTM, and to other relevant fora.

1.2 References

[1] DEPARTMENT OF TRANSPORTATION Federal Aviation Administration 14 CFR Parts 1, 47, 48, 89, 91, and 107 [Docket No.: FAA–2019–1100; Notice No. 20–01] RIN 2120–AL31 Remote Identification of Unmanned Aircraft Systems

[2] ASTM F3411-19, “Standard Specification for Remote ID and Tracking”

[3] 3GPP TS 22.125 “Unmanned Aerial System (UAS) support in 3GPP; 3rd Generation Partnership Project; Stage 1”

[4] 3GPP TR 23.754 “Study on supporting Unmanned Aerial Systems (UAS) connectivity, Identification and tracking (Release 17)” ()

[5] 3GPP TS 23.401 “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”

[6] 3GPP TS 23.501 “System architecture for the 5G System (5GS)”

[7] 3GPP TS 23.502 “Procedures for the 5G System (5GS)”

[8] 3GPP TS 23.256 “Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2 (Release 17)”

[9] 3GPP TS 23.288 “Architecture enhancements for 5G System (5GS) to support network data analytics services”

[10] 3GPP TS 23.003 “Numbering, addressing and identification”

[11] ACJA WT3 LTE Aerial Profile (link)

[12] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (Text with EEA relevance) C/2021/2671

1.3 Terminology and Abbreviations

Acronym	Explanation
3GPP	3rd Generation Partnership Project
5GS	5G System
BRID	Broadcast Remote ID
EASA	European Union Aviation Safety Agency
EPS	Evolved Packet System
FAA	Federal Aviation Administration
GCS	Ground Control Station
GMLC	Gateway Mobile Location Center
GPSI	Generic Public Subscription Identifier
LCS	Location Services
LEA	Law Enforcement Agency
MCN	Mobile Core Network
MNO	Mobile Network Operator
MSISDN	Mobile Subscriber ISDN Number
NEF	Network Exposure Function
NRID	Networked Remote ID
PDN	Packet Data Network
PDU	Packet Data Unite
PEI	Permanent Equipment Identifier
RID	Remote Identification / Remote ID
SCEF	Service Capability Exposure Function
SUPI	Subscription Permanent Identifier
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System (referred in 3GPP as Uncrewed Aerial System)
UAV	Unmanned Aerial Vehicle (referred in 3GPP as Uncrewed Aerial Vehicle)
UAVC	UAV Controller
USS	UAS Service Suppliers
UUAA	USS UAV Authentication & Authorization

2. Background on UAS Regulatory Requirements for Remote Identification and Lawful Intercept

This section focuses on requirements related to Remote Identification and is not to be considered exhaustive of all requirements and regulations related to UAS.

2.1 Remote Identification

Drones or unmanned aircraft systems (UASs) are fundamentally changing aviation, and regulatory bodies (e.g., FAA, EASA) are working to fully integrate drones or UAS into the National Airspace System (NAS).

UAS Remote Identification is the ability of a UAS in flight to provide identification information that can be received by other parties. RID is not for C2 (command and control). Remote ID has been designed to help facilitate more advanced operations for UAS and lay the groundwork for future UAS Traffic Management (UTM). In the scope of this document, we refer to Remote ID USS when mentioning USS, unless explicitly stated.

Remote ID assists the regulatory agencies, flight control agencies, law enforcement (e.g. GCS is an FBI/police terminal), and Federal security agencies identify when a UAS appears to be flying in an unsafe manner or where the drone is not allowed to fly.

Remote ID USS has four primary functions:

- Share RID in real-time over internet.
- RID access security.
- Meet contractually established parameters.
- Inform UAS status to government agencies (e.g. FAA), such as using one-time session ID for communication with government agencies.
- ICAO does not prescribe any RID equipage for UAS, but material under development addresses UTM and UAS operations under IFR.

The RID model includes:

- Broadcast Remote ID (BRID): method to identify UAS operating nearby by having the UAV broadcast a signal that can be interpreted by other UAVs and by GCS (Ground Control Stations). Currently BRID is over Wi-Fi or Bluetooth with limited range imposed by the underlying technologies. ACJA is interested in applying cellular technologies for the support of BRID (i.e. PC5) to enable longer ranges. BRID of course does not work over

longer distances, is not persistent, and does not contain information about flight plan or operational intent. BRID is not dependent on network coverage.

- Networked Remote ID (NRID): operators (MCN) connect to one of many Remote ID UAS Service Suppliers (USS) authorized by regulatory agencies (e.g. FAA), who serve as middleman between the MCN and the regulatory agencies via an API defined by regulators. An interface between MCN and the Remote ID USS would be defined (in scope of 3GPP). Multiple parties can populate data (coverage, flight paths, traffic, geofencing, etc., possibly for category of flight and of UAV) and consume data (UAV location, UAV behavior).

The information related to the Remote Identification include:

Table 2.1-1: Remote Identification information

Type	Content	Applicability	Optional/ Mandatory
UAS Identification (UAS ID)	Unique identifier of the UAS: This should be specific to the UAS, continuously available in near real time, electronically and physically readable, tamper resistant, and easily accessible.	BRID/NRID	M
	Identifying information of the UAS owner and remote pilot: This information would not be broadcast or published, but would be available from UTM system	NRID	M
UAV Flight Information	Tracking information for the UAV: This should include aircraft position and control station location (or takeoff location if ground control station location is not available)	BRID/NRID	M
	Mission type: This characterizes the flight path of the UAV	NRID, BRID?	O
	Route data: This includes pre-programmed navigation or flight plans	NRID, BRID?	O
	Operating status of the UAV: This refers to operational information that may provide some insight into the current operations of the UAV	NRID, BRID?	O

For Remote Identification, two components should be considered separately:

- Identification: information necessary for a receiver to identify the UAV or retrieve the complete set of identification information for the UAV (e.g. Identifying information of the UAV owner and remote pilot)
- Flight Information: this includes the set of information that the UAV broadcast regarding flight (e.g., location, altitude, speed, direction, etc.).

NOTE: It is assumed that such information and its security is fully transparent to the 3GPP system in terms of content.

Two categories of remote identifications are considered:

- Standard Remote Identification UAS (i.e., NRID in USA): a UAS with remote identification equipment capable of both:

1. Connecting to the internet and transmitting through that internet connection to a Remote ID USS; and

2. Broadcasting directly from the UAV.

Any person operating a standard remote identification UAS would be required to ensure:

- that the serial number of the standard remote identification UAS is listed on a declaration of compliance accepted by the government agencies (e.g., FAA). The standard remote identification UAS broadcasts the remote identification message elements directly from the UAV from takeoff to landing.
- When the internet is available at takeoff, the standard remote identification UAS connects to the internet and transmits the required message elements through that internet connection to a Remote ID USS.

The required message elements include, among others, a UAS Identification to establish the unique identity of the UAS.

- either the serial number of the UAV
- or a session ID (e.g., a randomly generated alphanumeric code assigned by a Remote ID USS on a per-flight basis designed to provide additional privacy to the operator)

A person can operate a standard remote identification UAS only if:

1. It has a serial number that is listed on a declaration of compliance accepted by the government agencies (e.g., FAA);

2. its remote identification equipment is functional and complies with the requirements of the proposed rule from takeoff to landing; and

3. its remote identification equipment and functionality have not been disabled.

Limited Remote Identification UAS: a UAS with remote identification equipment capable of only Connecting to the internet and transmitting through that internet connection to a Remote ID USS.

2.2 FAA Remote Identification

2.2.1 Overview

The following is a summary of the Federal Aviation Administration (FAA) published rule for Remote Identification (RID) [1] for UAS.

Safety and security are top priorities for the FAA (and U-Space of EASA) and Remote Identification (Remote ID-RID) of UAS is crucial to the integration efforts.

Remote Identification is introduced to be deployed in conjunction with UAS Service Suppliers (USS) in the scope of UTM, and the FAA envisions that third parties will supply USS and UTM services.

The main “elements” included in the FAA proposal for Remote Identification are:

- UAS owners.
- UAS operators.
- UAS designers/producers.
- Developers of RID (compliance to FAA, this proposal).
- Remote ID USS.

The work in [1] partially results from the UAS Identification and Tracking Aviation Rulemaking Committee (ARC), chartered by the FAA in June 2017, which submitted its report and recommendations to the agency on technologies available to identify and track drones in flight and other associated issues. Remote Identification Model

Note that **the FAA published rule [1] on Remote ID has excluded Networked Remote ID**.

The owners of standard remote identification UAV (i.e., capable of broadcast and network connectivity) or limited remote identification UAV (capable only of network connectivity and not allowed to fly over 400ft) would have to provide the serial number of all registered UAV. The serial number would establish the unique identity of the unmanned aircraft.

The FAA is requesting to require standard remote identification UAS to use the same remote identification message elements, including the same UAS Identification, when transmitting to a Remote ID USS and broadcasting directly from the UAV.

Remote ID USS would be required to demonstrate four primary capabilities:

1. The ability to share the remote identification message elements in near real-time with the FAA upon request.
2. the ability to maintain remote identification information securely and to limit access to such information.
3. the ability to meet contractually- established technical parameters; and
4. the ability to inform the FAA when their services are active and inactive.

Another capability of a Remote ID USS may be to generate and provide UAS operators with a UAS Identification known as a session ID.

2.2.2 UAS Serial Number

The FAA and the European Commission are requesting UAS manufacturers to use ANSI/CTA–2063–A standard to define the UAS serial number.

2.2.3 Spectrum

The FAA is requesting to require that standard remote identification UAS be capable of broadcasting the message elements using a non-proprietary broadcast specification and radio frequency spectrum in accordance with 47 CFR part 15 that is compatible with personal wireless devices. The FAA envisions that remote identification broadcast equipment would broadcast using spectrum similar to that used by Wi-Fi and Bluetooth devices. The FAA is not, however, proposing a specific frequency band. Rather, the FAA envisions industry stakeholders would identify the appropriate spectrum to use for this capability and would propose solutions through the means of compliance acceptance process. This requirement would ensure that the public has the capability, using existing commonly available and 47 CFR part 15 compliant devices, such as cellular phones, smart devices, tablet computers, or laptop computers, to receive these broadcast messages.

2.2.4 Remote Identification Message Elements

The message elements for limited remote identification UAS would include:

1. The UAS Identification.

The UAS Identification message element establishes the unique identity of UAS operating in the airspace of the United States. This message element would consist of one of the following:

- **A serial number** assigned to the unmanned aircraft by the person responsible for the production of the standard or limited remote identification unmanned aircraft system.

  FAA selected the serial number assigned at manufacturing instead of an UAV registration number because it is a unique identifier issued by the UAS producer to identify and differentiate individual aircraft and encoded into the UAV system during production; on the contrary, a registration number is provided to the owner of the UAV and may change for that aircraft if the UAV is resold. In addition, a registration number is assigned by the FAA only after a UAS owner applies for one, whereas a serial number would be assigned prior to the UAS being purchased and would provide a means for the UAS to send out a remote identification message, even if it is not registered. The FAA anticipates a UAS would be designed to broadcast and transmit, as appropriate, its serial number regardless of whether the UAV has been registered or not.

- or a session identification number (**session ID**) assigned by a Remote ID USS.

  The association between a given session ID and the UAV serial number would not be available to the public through the broadcast message. This association would be available to the issuing Remote ID USS, the FAA, and other authorized entities, such as law enforcement.

2. An indication of the control station's latitude and longitude derived from a position source, such as a GPS receiver. The FAA notes that it is not proposing a specific type of position source

used to determine this information to allow the greatest flexibility to designers and producers of UAS.

3. an indication of the control station's barometric pressure altitude, used to establish a standard altitude reference for UAS operating in the airspace of the United States and provide information that could be used to approximate the control station's height above ground level

4. a time mark, identifying the Coordinated Universal Time (UTC) time of applicability of a position source output.

5. an indication of the emergency status of the UAS that indicates the emergency status, which could include lost-link, downed aircraft, or other abnormal status of the UAS. The FAA anticipates that a standard for remote identification would specify the different emergency codes applicable to UAV affected by this rule. This message element could be initiated manually by the person manipulating the flight controls of the UAS or automatically by the UAS, depending on the nature of the emergency and the UAS capabilities. This message element would alert others that the UAS is experiencing an emergency condition and would indicate the type of emergency.

The message elements for standard remote identification UAS would include the same message elements required for limited remote identification UAS plus:

1. an indication of the UAV's latitude and longitude: derived from a position source, such as a GPS receiver. This message element would be used to associate a specific UAV with its associated control station position. It would also be used to provide situational awareness to other aircraft, both manned and unmanned, operating nearby. Manned aircraft, especially those operating at low altitudes where UAS operations are anticipated to be the most prevalent, such as helicopters and agricultural aircraft, could carry the necessary equipment to display the location of UAS operating nearby. Facility operators could use latitude and longitude information to know about the location of UAS operating near an airport, airfield, or heliport.

2. an indication of the UAV's barometric pressure altitude, used to establish a standard altitude reference for UAS operating in the airspace of the United States. The FAA considered and rejected a requirement to indicate the UAV's geometric altitude, concluding that a single altitude reference—barometric pressure altitude—is sufficient (see discussion in XII.C.3 of this preamble). The FAA requests comments regarding whether both barometric pressure altitude and geometric altitude of the UAV should be part of the remote identification message elements.

2.2.5 Performance requirements:

The following requirements apply to Remote Identification:

- Tamper Resistance: the FAA is requesting in §89.310(e) for standard remote identification UAS and in §89.320(e) for limited remote identification UAS to require that UAS with remote identification be designed and produced in a way that reduces the ability of a person to tamper with the remote identification functionality.

- Connectivity:

  - Remote ID message elements are required to be broadcast directly from the UAV.
  - Interference Considerations: prohibit the remote identification equipment from causing harmful interference to other systems or equipment installed on the UAV or control station (e.g., to the UAS command and control datalink).
  - Positional Accuracy: for standard remote identification UAS, the reported position of the UAV and control station would have to be accurate to within 100 feet of the true position, with 95 percent probability. For limited remote identification UAS, the same requirement is proposed except that it would only apply to the control station. The proposed 100-foot accuracy requirement is based on the 30-meter (98.4 feet) accuracy requirement for commercial off the shelf GPS position sources allowed for Traffic Awareness Beacon System (TABS) equipment in TSO–C199.
  - Barometric Pressure Altitude Accuracy: for standard remote identification UAS, the reported barometric pressure altitude for the UAV and the control station would be required to be accurate to within 20 feet of the true barometric pressure altitude for pressure altitudes ranging from 0 to 10,000 feet. For limited remote identification UAS, the same requirement is proposed for the control station only
  - Remote Identification Message Latency: a latency of no more than one second is required. This would apply to both the transmitted message set and the broadcast message set and is the time between when a position is measured by the UAV or control station position source and when it is transmitted and broadcast by the remote identification equipment. This does not apply to any systems external to the UAS, such as broadcast receivers or information display devices
  - Remote Identification Message Transmission Rate: a transmission rate of at least 1 message per second (1 hertz) is required and applies to both the message elements transmitted to a Remote ID USS and broadcast.
  - Range Limitation: a limited remote identification UAS must be designed to operate no more than 400 feet from its control station.

2.2.6 Applicability of Remote ID and Tracking Requirements

Option1: All UAS are required to comply with remote identification and tracking requirements except under any of the following circumstances:

- The UAV is operated within visual line of sight of the remote pilot and is designed to not be capable of flying beyond 400 feet of the remote pilot.
- The UAV is operated in compliance with 14 CFR part 101, unless the UAV: Is equipped with advanced flight systems technologies that enable the aircraft to navigate from one point to another without continuous input and direction from the remote pilot; or is equipped with a real-time downlinked remote sensor that provides the remote pilot the capability of navigating the aircraft beyond visual line of sight of the remote pilot.
- The UAS is operated under ATC and contains the equipment associated with such operations (including ADS–B, transponder, and communication with ATC).
- The UAS operation is exempt from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security, defense, or under an FAA waiver).

Option 2: UAS with either of the following characteristics are required to comply with remote identification and tracking requirements:

- Ability of the aircraft to navigate between more than one point without direct and active control of the pilot.
- Range from control station greater than 400 feet and real-time remotely viewable sensor.
- The ARC also recommended that, regardless of which option for applicability the FAA chooses, UAS operating under the following circumstances be exempt from the remote identification and tracking requirement:
- The UAS is operated under ATC and contains the equipment associated with such operations (including ADS–B, transponder, and communication with ATC).
- The UAS operation is exempt from ID and tracking requirements by the FAA (e.g., for the purposes of law enforcement, security, or defense, or under an FAA waiver).

2.2.7 Remote ID USS for Networked Remote ID

The FAA does not propose to require a Remote ID USS be universally compatible with all UAS. That said, the FAA anticipates that some UAS manufacturers will also be Remote ID USS. In those cases, the Remote ID USS may choose to only connect to UAS made by the same manufacturer. This model is similar to how mobile telephone networks sell devices that can only be used on their networks. The FAA requests comment on whether manufacturers should be permitted to produce UAS that are only compatible with a particular Remote ID USS.

Whether NRID is an acceptable mean of compliance for regular is unclear.

2.3 EASA Remote Identification

European Regulation addresses both Broadcast and Network RID. In Europe, Remote ID is imposed to all UAV except a few super light UAV.

There are three categories of operations: OPEN, SPECIFIC and CERTIFIED

- For drones operating in the OPEN category
- direct remote ID (equivalent to Broadcast Remote ID) is imposed
- network remote ID is an option (in case they need to operate in U-Space)

All drones operating in the open category needs to be CE (“Conformité Européenne”) marked; the related requirements can be found in the Delegated Regulation (EU) 2019/945 updated by (EU) 2020/1058 - refer for instance to ANNEX TO DELEGATED REGULATION (EU) 2019/945 Part 2 requirements sub-paragraphs (12) for direct and (20) for N-ID.

- For drones operating in the SPECIFIC category, Commission regulation (EU) 2020/1058 Article 40(5) demands that all UAS intended to be operated in the specific category at a height of less than 120m are equipped with remote identification (direct remote ID is not imposed; the manufacturer could choose to use Network ID instead).
- U-Space regulation [11] is imposing N-ID for all users; this is summarized in recital of the Implementing Regulation (EU) 2021/664: "UAS operators should operate in U-space airspace only if they make use of the U-space services that are indispensable to ensure safe, secure, efficient and interoperable operations. U-space service providers should provide at least the following mandatory U-space services: a network identification service, a geo-awareness service, a UAS flight authorisation service and a traffic information service."

2.4 Networked Remote ID

In scenarios in which Networked Remote ID is either used as an alternative mean of compliance to the current FAA rule or as a future extension of the FAA rule, or to scenarios where NRID is mandated, the following applies:

- Automatic Remote ID USS Connection: from takeoff to landing, the UAS would be required to automatically maintain a connection to the internet when available and would be required to transmit the message elements to a Remote ID USS through that connection. The FAA envisions that UAS would connect to an internet-based Remote ID USS upon initialization. The FAA welcomes comments on whether the connection should be required from takeoff to landing or whether it should be required from start up to shut down.
- Connectivity:
  - If the internet is available at takeoff, the UAV would be required to be designed and produced so that it would not be able to take off unless it is connected to the internet and transmitting the message elements through that internet connection to a Remote ID USS.
  - In addition, if the internet is unavailable at takeoff, the standard remote identification UAS would not be able to take off unless it is broadcasting the message elements.
  - A standard remote identification UAS is required to continuously monitor its connection to the internet and the transmission of remote identification message elements to a Remote ID USS. If either is lost, the UAS would have to notify the person manipulating the flight controls of the UAS so he or she may take appropriate action, as needed. For limited remote identification
  - If the internet is unavailable at takeoff, the limited remote identification UAS would not be able to take off because, unlike a standard remote identification UAS, a limited remote identification UAS would not be able to broadcast the remote identification message elements.

2.5 Lawful Interception (LI)

3GPP systems have Lawful Interception capabilities independent of Remote Identification aspects and applicable to any mobile device, by which an MNO can, based on warrant received from Law Enforcement Agency (LEA):

- Provision the target identity in the network to enable isolation of target communications (separating it from other users' communications)
- Duplicate the communications for the purpose of sending the copy to the LEA
- Handover the Interception Product to the LEA

The existing LI capabilities are assumed to be sufficient for UAS regulatory requirements related to lawful interception as well.

3. Clarification of Scope

3.1 3rd Generation Partnership Program (3GPP)

The scope of 3GPP work with respect to UAVs includes:

- identify, based on (aerial) subscription, that the UE is used with an UAV
- identify if connectivity service requested by the UAV UE will be used for UAV operations

The 3GPP system provides connectivity services for C2 communication and other UAV operations and additionally may also provide other potential services like location, tracking, reporting of the UAVs, with required Quality of Service (QoS).

The 3GPP system may expose services towards the USS/UTM for a secondary authentication/authorization of the UAV, however, 3GPP system is not involved in the actual authentication/authorization process and even may not be aware of various information exchanged between the UAV and the USS/UTM (e.g., identities, flight path information etc.) for such authentication/authorization. The 3GPP system may, however, be aware of the outcome of such authentication/authorization done by the USS/UTM and may even limit (under control of the USS/UTM via the 3GPP NEF webservices) the connectivity services provided to UAV UEs when not authenticated/authorized by USS/UTM.

3GPP system may expose various services to systems like USS/UTM/TPAE (Third Party Authorized Entity, e.g., police) via NEF web services framework, through a set of well-defined APIs standardized by 3GPP. Services exposed by 3GPP system shall be accessed using a 3GPP level identifier.

3GPP system may provide necessary information related to location or tracking of a UAV UE, when requested by an external entity e.g., USS, however, 3GPP system on its own does not monitor any air traffic or does not do any policing or tracking of the UAVs.

When 3GPP connectivity is used for command and control (C2) communication with the UAV, the actual C2 messages exchanged between the UAV and the UAV controller, or a ground control station is transparent to the 3GPP system as it happens on the user plane at the application level. Thus, the 3GPP system does not have any control on the actual messages exchanged for C2

The following aspects are outside the scope of 3GPP work:

- The allocation/management of UAV identities used for remote identification of UAVs (e.g., format of the identifier, how it is provisioned in the UAV and so on)
- Security solutions for privacy of the Networked Remote ID (NRID) communication between UAV and USS. Security aspects will be studied at ACJA WT1 and documented in clause **Error! Reference source not found.** of this document

3.2 USS provider

In the scope of this document, USS refers to both a generic USS and a Remote Identification USS.

Identification & Authentication/authorization of the UAV for USS services are done between the USS and UAV. 3GPP system may provide connectivity/transport mechanism to transfer related messages between UAV and USS and should be able to also request the outcome of the authorization from the USS.

Authentication/authorization of the UAV Controller (UAVC) is outside the scope of the current document. UAVC may or may not establish a connection to the 3GPP system and/or the USS.

The USS may request location services for a UAV when the GPS location services are unavailable.

The USS may interface with the configuration/subscription management service exposed by MNO for UE activation/deactivation. This may be optionally required when the USS is owned by the MNO. This feature is optional and provides a tool usable subject to regulations in various regions.

The USS may interface with network resource management services exposed by the MNO, to manage Quality of Service (QoS). This may be optionally required when the USS is owned by the MNO.

The UAV will identify to the USS through a UAS ID which may consist of the UAS serial number, or a session ID provided by the USS. The USS will be able to map the UAS ID to the 3GPP identity.

The USS may choose to supply services for UAV to UAVC pairing, but that is out of the scope of current document.

USS may be queried to supply information to third party authorities about a UAV/UAS, but all necessary information should be retained by the USS without needing to query 3GPP system.

4. Overall Architecture for UAS Enablement via 3GPP Systems

The following section applies to MNOs acting as SDSPs (Supplementary Data Service Providers of the UTM model) and is not meant to be interpreted as applying to SDSPs in general.

4.1 ACJA Reference Architecture

This section identifies the functional entities related to the enablement of UAS operations via 3GPP systems and the support of UAV Remote Identification.

4.1.1 Identification of Roles

Table 4.1.1-1: Function for UAV Identification (source 3GPP)

Functions	UAS Operator	USS	MNO (SDSP)	UAS OEM	CAA	TPAE (public Safety)
Assignment of UAV SN (CTA-2063-A)				P		
Assignment of CAA-level UAV ID					P	
Assignment of UTM UUID		P for USS ID	S (O)			
Assign flight operation “USS ID/CAA-level UAV ID” (1)		P for USS ID	S (O) for USS ID		P for CAA-level UAV ID	
Assign 3GPP MNO UAS ID			P			
Map USS ID/CAA-level UAV Identity to 3GPP MNO UAS ID, etc		P	S			
Manage UAS and Operator IDs (pilot, UAV SN, etc.) in terms of registration of UAS		S	Not involved		P	

Meaning of symbols: P: primary; S: secondary, supports primary role;?: FFS; O: optional

Notes:

(1) It is assumed that the identifier used in BRID and NRID is the “USS ID/CAA-Level UAV Identity”.

Note that no assumption is made with respect to the relationship between the Remote ID USS and the MNO.

Whether the UAS OEM is indicative of both the UAV and the GCS, or only the UAV, is FFS.

Table 4.1.1-2: Function for UAV Authorization/Authentication (source 3GPP)

Functions	UAS Operator	USS/SDSP	MNO	UAS OEM	CAA	TPAE (public Safety)
Associate (“register”) UAS with UTM	S	P			S	
Verify validity of UAS registration (CAA-Level UAV Identity) with CAA		P	S (1)/O			
Authenticate UAS hardware	S	P (2)	S (3)/O	S	S	
Authenticate UAV aerial subscription			P			
Authorize and association UAV and GCS/UAV Controller		P/O	S/O		S	
Authorize aerial services after authentication (4)		P	S/O			

Notes:

(1) This is part of the UAS authorization/authentication function defined in 3GPP

(2) This applies to UAS-USS interactions, may be based on verifying hardware validity

(3) This applies to ensuring the UAV accessing a 3GPP system is authorized by CAA and USS

(4) In this case authorization refers to the USS indicating to the MNO that the UAS is authorized to obtain to what 3GPP has defined as aerial services (and documented in [11]).

Table 4.1.1-3: Function for Control of connectivity between UAV and USS and UAV and GCS/UAV Controller (source 3GPP)

Functions	UAS Operator	USS	MNO (SDSP)	UAS OEM	CAA	TPAE (public Safety)
Enable(1) UAV-USS connectivity (optional)			P (2)/O			
Enable(1) UAV-GCS/UAV Controller connectivity (optional)		P (3, 4)	S (3, 4)/O			

Notes:

(1) The USS authorizes the UAS to gain connectivity as a UAS that is registered with CAA and an USS, and not a rogue unauthorized UAS. This is done at UEs subscription level. If this is an aerial UE, then access to certain DNN/S-NSSAI is allowed only after the 3GPP confirms that the UAV is registered and authorized. If the UAV is not authorized, the UE may be allowed to access other DNN/S-NSSAI that are not related to UAS services.

(2) Assumed to be available by default based on aerial subscription

(3) It is assumed that connectivity is available only if authorized by USS, and that restricting such connectivity is a mechanism used by USS/MNO to handle misbehaving UAS. This applies only to networked UAVs.

(4) This includes enabling the connectivity upon UAS request, modifying it upon USS or UAS request, and removing/restricting it upon USS request.

Table 4.1.1-4: Function for geoawareness services provided by an MNO (source 3GPP)

Functions	UAS Operator	Remote ID USS	MNO (SDSP)	UAS OEM	CAA	TPAE (public Safety)
Provide network-based location services			P			
Monitor UAS location (1)	S	P	S/O			
Geoawareness before takeoff (1)	S	P	S/O			
Geoawareness after takeoff (1, 2)	S	P	S/O			

The assumption is that the MNO provides geoawareness to enable the enforcement by USS of geocaging and geofencing. This is not assumed to be a mandatory functionality.

Notes:

(1) It is assumed that though the UAS operator is obviously monitoring the UAS location, it is the USS that is responsible for tracking it.

(2) This includes identifying, managing, and sharing airspace and geofences

4.1.2 Overall Architecture and Assumptions

The content of this section applies to the architecture for connectivity and services defined by 3GPP for Release 17 [8]. Some components are optional in specific implementations.

It is assumed that a UAS will be identified either before connecting with the 3GPP system or using plain internet connectivity via the 3GPP system. The UAS ID may take several formats to support various geo-specific regulations, including Serial Number Identification, a CAA-level UAV ID (aka Registration ID), and USS/UTM-Issued UUID (aka “session ID”).

When a UAV requests for UAS services (i.e., to take advantage of 3GPP RAN aerial features, connectivity with USS/UTM for Networked Remote Identification, and C2 connectivity) it also provides the CAA-Level UAV ID and aviation level information to 5GS or EPS. The aviation level information is transparent to the 5GS/EPS. A UAV that has not performed a registration with CAA authorities does not attempt to request for UAS services from the 3GPP system.

Two types of connectivity are supported: single PDU session/PDN connection for connectivity between the UAV and the USS and for connectivity between the UAV and the UAVC connectivity, and separate PDU sessions/PDN connections for USS and UAVC connectivity. The mechanism that may be used is up to deployment.

The UAV is allowed to establish connectivity with an appropriate DNN/APN to exchange traffic with the USS (i.e., for communications not related to sending Remote Identification message or C2) based on MNO policies and without explicit USS/UTM authorization for the establishment of the user place connectivity.

An UAV is identified by USS using a UAS ID and identified by the 3GPP System using a 3GPP UAV ID (e.g., GPSI) assigned by the MNO. However, the USS is also provided the 3GPP UAV ID of the UAV for the USS-MNO interfacing for service exposure.

The UAS ID ID is used for Remote ID functionality (network or broadcast remote ID). Remote Identification support by 3GPP in the scope of this release applies to the UAV, not to UAV Controller. No assumptions are made limiting the type of information on UAV Controller can provide via Remote Identification to satisfy regulatory requirements.

The 3GPP system requires information about the USS to trigger authentication/authorization requests for the UAV that is requesting UAS services from the 3GPP system. It is assumed that the mechanisms for resolution of UAS ID to the USS serving the corresponding UAV, defined outside 3GPP, and available to entities outside the 3GPP system (e.g., the TPAE), are used in the 3GPP system to discover the USS for the UAV.

It may be also possible to use other UAV information (e.g., UAV-provided USS address or domain name) sent by the UAV to 3GPP system, to be used by the 3GPP System, to discover the USS for the UAV.

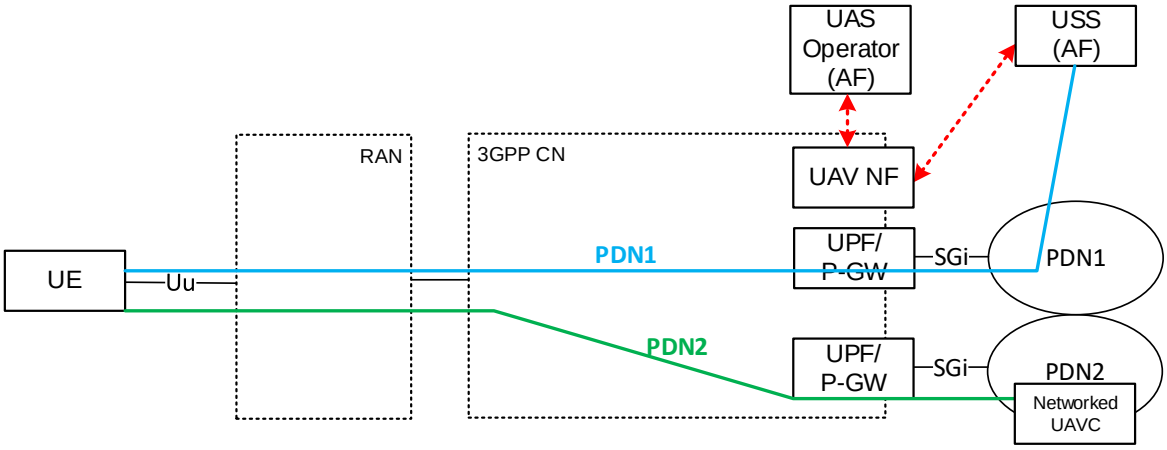

Figure 4.1.2-1: ACJA Reference Architecture

The UE (UAV) connectivity is based on PDN connections (in 4G systems) and PDU sessions (in 5G systems) which provides a connection to a packet data network, as described in the appendix.

As described above, the UAS NF interfaces with the USS to provide a variety of services available to the USS for the support of UAVs:

- enable UAV authentication/authorization

- for a UAV to get access to 3GPP services for C2 connectivity and for Networked Remote ID, the UAV must be authenticated/authorized as a valid UAV by the USS. The complexity of such authentication/authorization depends on mechanisms defined outside 3GPP.
    - The 3GPP systems provides mechanisms to support an authentication/authorization procedure between the UAV and the USS/UTM. During this procedure, the USS/UTM may access additional information from the 3GPP system (e.g., UAV location) to decide about the authentication/authorization and provides information about the result of the authentication/authorization.
    - During the UAV authentication/authorization procedure, the 3GPP system provides 3GPP identities/information for the UAV including the GPSI, optionally the PEI, the UAS ID and any aviation level information the UAV has provided to the 3GPP system. The USS/UTM uses such information for the authentication/authorization and for future interactions with the 3GPP system regarding the UAV via NEF/SCEF.
- enable UAV flight authorization
    - Prior to any request by UAV for user plane connectivity with UAVC, or during the user plane connectivity request, the UAV must obtain flight authorization from the USS, and the results must be made known to the 3GPP system in order to authorize the connectivity.
    - Flight authorization from the USS, when performed during the user plane connectivity request, must minimize the amount of information exchanged between the UAV and the USS in an Aviation Connectivity Payload transferred between the UAV and the USS transparently to the 3GPP system. This can e.g., be achieved by the UAV operator obtaining offline a Flight Authorization ID from the USS via means outside the scope of 3GPP, and having the UAV provide the Flight Authorization ID in the PDU session/PDN connection establishment.
- enable UAV-UAVC pairing authorization
    - the 3GPP system supports the optional USS authorization of pairing between a UAV and a networked UAVC, or a UAVC that connects to the UAV via Internet connectivity during the establishment of the PDN connection/PDU session for UAS services (i.e., connectivity to USS/UTM and for C2 traffic). Modifications or establishment of the pairing or re-authorization take place via modification of the established PDN connection/PDU session. During such procedures, and during the establishment of connectivity for C2, the USS provides to the 3GPP system information (e.g., QoS requirement, data flow descriptors, etc.) that enable traffic between the UAV and the UAVC. How the USS is made aware of the UAVC is not defined by 3GPP and is assumed to take place via application layer data exchange between the UAV and the USS.
- enable revocation of authorizations
    - UAV authorization and authentication may be revoked by the USS at any time by invoking MNO services (e.g., exposure function or location services) by using the 3GPP UAV ID and providing a Revocation Cause indicating this is authorization and authentication revocation.
    - Authorization for C2 connectivity and UAV and UAVC pairing may be revoked by the USS at any time by invoking MNO services (e.g., exposure function or location services) by using the 3GPP UAV ID and providing a Revocation Cause indicating this is C2 or pairing revocation.
- enable UAV tracking and MNO reporting to USS of the UAV location

- enable control of QoS/traffic filtering for C2 communication

The 3GPP system uses Web APIs to reach the USS serving a UAV (based on the UAS ID), and the USS can request services from the 3GPP system via queries, identifying the UAV using a 3GPP UAV ID, as described below.

4.1.2.1 Architecture Aspects

4.1.2.1.1 USS-MNO relationship

No commercial relationship is assumed between the 3GPP MNO and a USS in terms of the 3GPP MNO having to be informed of the USS serving a UAV a priori, so that an UAS operator may change the serving USS while remaining with same 3GPP Network subscription, and vice versa. The 3GPP Network subscription for the UAV is not assumed to contain any information about the USS/UTM based on a commercial relationship between the MNO and the USS/UTM.

However, it is possible that some level of service level agreement between the MNO and the USS may be needed, in order to enable the MNO to expose network services securely to the USS.

4.1.2.1.2 Pairing between UAV and networked UAVC

The 3GPP system makes available to a USS an optional functionality to support authorization of UAV and UAVC (i.e. GCS) pairing, which applies to networked UAV Controllers and non-networked UAV controllers that are connected to UAV via internet (e.g. cloud UAVC).

The 3GPP system does not define how a UAV and a UAVC are considered as a UAS by the USS, but the 3GPP system supports the USS to enforce authorization of pairing a UAV and a UAVC based on their transport addresses.

The UAV/UAVC pairing authentication and authorization is done by USS during establishment or modification of C2 connectivity (i.e. PDU session or PDN connection).

The UAV may provide information for the authorization of UAV and networked UAV controller pairing to the USS in the establishment or modification of C2 connectivity, and the USS informs the results of pairing authorization to the 3GPP system in terms of identification of the traffic that needs to be enabled.

As part of pairing authorization, the 3GPP system enables a UAV to receive a new UAS identifier from USS.

When the USS determines that the UAVC needs to be replaced, the USS provides new authorized UAV/UAVC pairing information to 3GPP system.

4.1.2.1.3 USS-MNO interfacing

For an external application function/server to address 3GPP services exposed to the function/server, the UAV to which the services relate must be identified via an identifier that the 3GPP network can recognize. We refer to this as 3GPP UAV ID, and it corresponds to the 3GPP GPSI assigned by the MNO to the UAV MNO subscription and is in the format of an External Identifier. When soliciting

services from the 3GPP network, the USS would use the 3GPP UAV ID associated to the UAV to identify the UAV, independently of how the USS identifies the UAV for its own functions. The External Identifier is allocated by the 3GPP network without interaction with the USS/UTM, and must be unique within the geography (e.g., at least country) of the 3GPP network.

It is expected that a 3GPP GPSI in the format of an MSISDN is not used for UAVs, similar to the case of IoT devices, for simplicity of managing UAV subscriptions.

4.1.2.1.4 USS awareness of UAV cellular connectivity

The USS is not assumed to have knowledge of PDU sessions or PDN connections: the USS/UTM authorizes connectivity requests sent from the 3GPP system for a UAV or UAV controller, can revoke such authorization, and can provide information to control such connectivity (e.g., ACL-Access Control List, QoS information, etc.). The USS shall not be required to be aware of whether the UAV uses a single PDN connection/PDU session for communication with USS and for C2 between the UAV and the networked/cloud UAVC, or whether separate PDN connections/PDU sessions are used for the two types of communications.

However, in case of single PDN connection/PDU session for communication with USS and for C2, the USS may receive simultaneous authentication/authorization requests for UAV flight authorization and UAV-UAVC pairing, whereas in the case of multiple PDN connections/PDU sessions for communication with USS and for C2, the authentication/authorization happens separately.

It is expected that the USS may be aware of QoS requirements for C2 connectivity and shall be able to provide such requirements to the 3GPP system.

4.1.2.1.5 UAV location and tracking

The UAV Tracking mechanisms made available to the 3GPP system are agnostic to the availability of Network Remote ID and provide location and tracking services to the USS based on 3GPP mechanisms.

Such mechanisms reflect what existing mobile networks can provide with respect to other UEs, and such tracking is enabled and consented to by having the UAV provide specific information to the 3GPP system that allows the 3GPP system to contact the USS, which in turn is capable of accessing the UAV location information.

The 3GPP system exposes a series of services to the USS for UAV Tracking. The following tracking options are possible:

- Immediate UAV location reporting: based on the request from USS, the 3GPP system provides the UAV location
- Periodic UAV location reporting: based on the request from USS, the 3GPP system provides the UAV location periodically, based on the interval negotiated between the USS and the 3GPP system
- Monitoring the UAV presence in the monitoring area (e.g. moving in or out of the monitoring area) and providing the monitoring report to USS. The USS subscribes for event monitoring for a specific UAV by providing an “Area of Interest”, in order to receive the reporting of UE presence in the monitoring area. The 3GPP system may maps the “Area of interest” to 3GPP

specific areas (e.g. cells) or may use the actual location based on 3GPP GMLC (Gateway Mobile Location Center) reporting.

- UAV discovery: the USS may provide an “area of interest” and receive from the 3GPP system the list of UAVs served by the 3GPP system and present in that specific area.

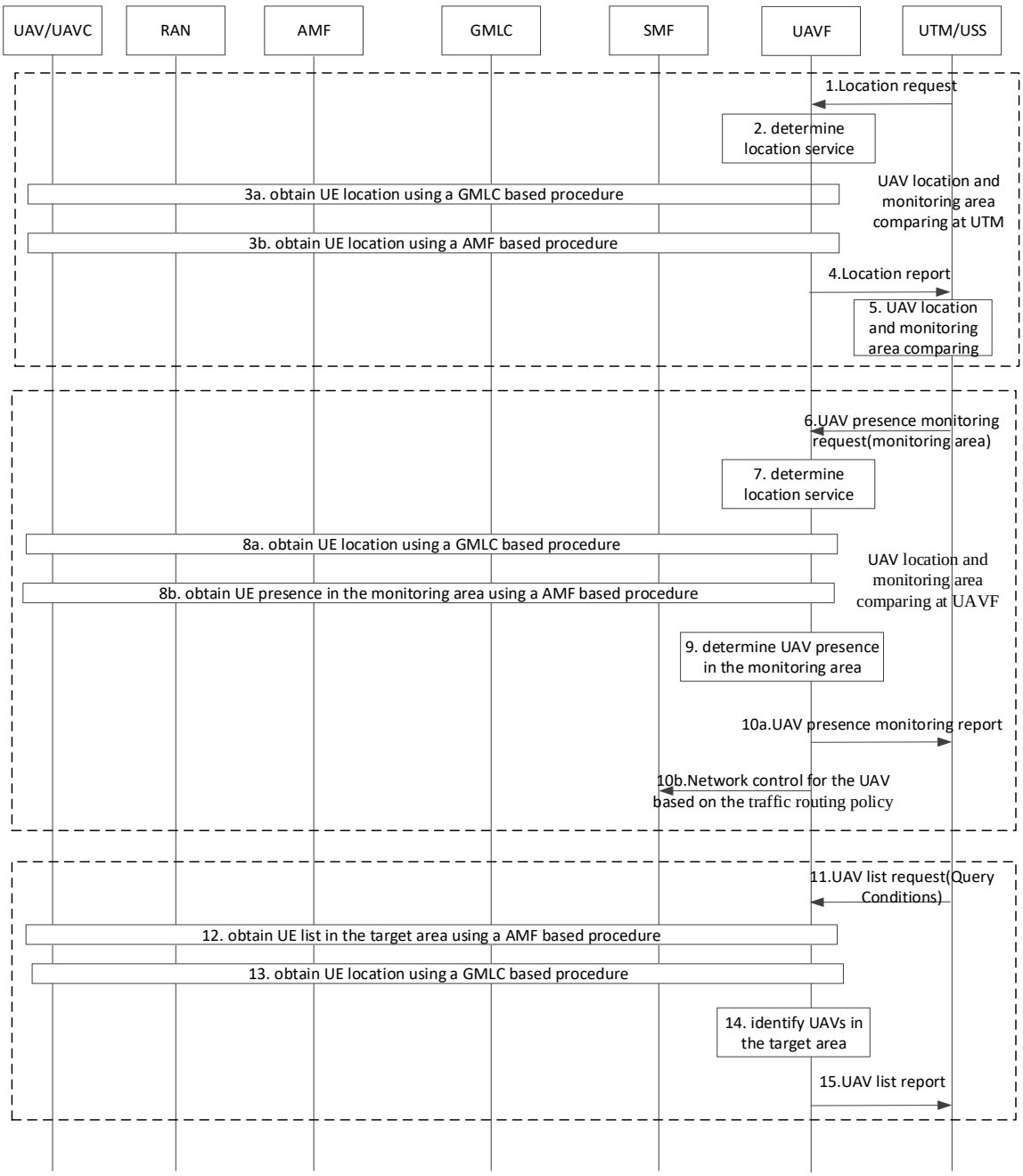

Figure 4.1.2.1.5-1: UAV Tracking Mechanisms.

It is assumed that UAVC tracking by USS is based on Networked Remote ID information, i.e., information reported to the USS by the UAV, and obtained by the UAV from UAVC with mechanisms outside the scope of 3GPP.

In order to support geofencing of UAVs by the USS, the 3GPP system enables both the “direct query from USS” model (where the USS queries the specific UAV location on demand), the “direct USS subscription” model (where the USS registers for UAV location reporting), and the “area of interest subscription” model (where the USS registers for reporting of events related to the UAV location with respect to a geographical area of interest indicated by the USS).

For geocaging, including ensuring a UAV is authorized to take off from approved locations, the 3GPP system supports both the option of the 3GPP system proactively providing the UAV location to the USS during authentication/authorization procedures, and the option where the USS retrieves it on demand, are supported.

4.1.2.2 Support of UAV Authorization in 3GPP Network

The 3GPP system is provided the UAS ID by the UAV, and it may provide the UAS ID to the USS in order to receive authorization from the USS for the UAV access to UAS services by the MNO.

The USS is made aware of the 3GPP UAV ID of the UAV during procedures of UAV authorization supported by the 3GPP network. The USS uses the 3GPP UAV ID to invoke MNO services (e.g., exposure function or location services) or during authorization or authorization revocation.

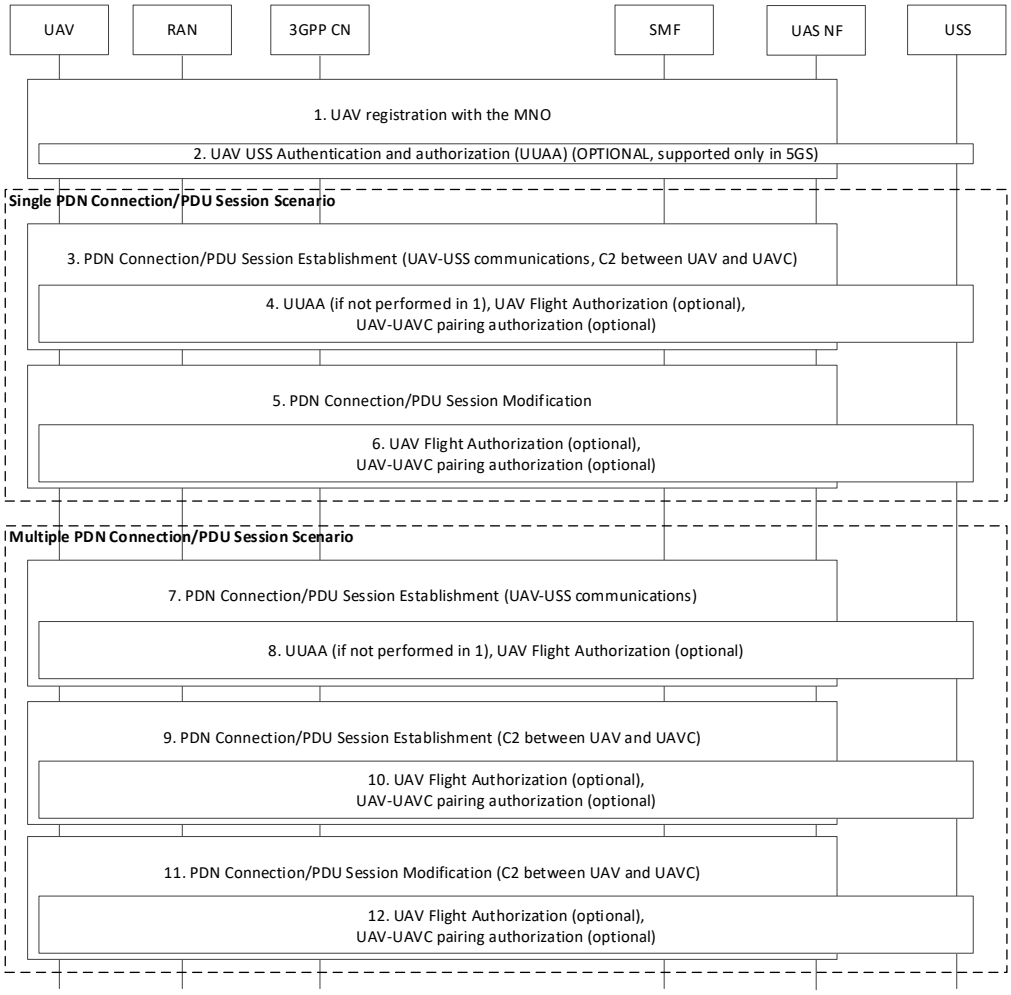

Figure 4.1.2.2-1: UAV Authentication and authorization in 3GPP system.

The model for the UAV authentication and authorization is based on the following:

- The 3GPP system enables the MNO to verify the validity of the UAV with the USS (i.e. whether the UAV is properly registered) via a UAV USS Authentication and Authorization procedure. An UAV is authenticated and authorized by USS/UTM via a USS UAV Authentication & Authorization (UUAA) with the support of the 3GPP system before connectivity for UAS services (e.g. UAS-USS connectivity for NRID) is enabled.

  Depending on 3GPP network operator and/or regulatory requirements, the UUAA is performed:

  - in 5GS: either as a separate procedure during the 5GS registration procedure, or when the UAV requests user plane resources for UAV operation (i.e. PDU session establishment). From a UE implementation point of view it is mandatory to support UUAA during Registration and PDU session establishment procedure. From a network deployment point of view it is mandatory to support UUAA during PDU session establishment procedure.

  - in EPS: during the attach procedure and the corresponding PDN connection establishment

A UAV that is in possession of a UAS ID provides the UAS ID in both 5GS Registration and in PDU Session/PDN Connection establishment. The CN determine whether UUAA is executed at 5GS registration or at PDU session/PDN Connection establishment based on local policies.

If UUAA is performed at Registration Procedure, the SMF serving the PDU Session for the UAV (e.g. the PDU session for UAV-USS connectivity and, if separate PDU sessions are used, the PDU session for C2 connectivity) is notified by the AMF of the successful UUAA.

If UUAA is not performed during the Registration procedure, the UUAA is performed at PDU session (or PDN connection) establishment when the UAV requests user plane resources for UAV operation and the UAV provides its UAS Id during PDU session (PDN connection) establishment.

When UUAA is performed at registration, the UAV flight authorization and UAV-UAVC pairing authorization is performed at PDU session/PDN connection establishment/modification procedures.

The execution of the USS UAV Authentication & Authorization during the registration procedure is optional and is based on specific PLMN policies, USS requirements, and geographic regulatory requirements.

- The 3GPP system enables the UAV to have a flight authorization by the USS by transparently delivering to the USS aviation information that the 3GPP system does not process. The 3GPP system only processes the result of the authorization and decides whether to enable the establishment of connectivity for C2 between a UAV and a UAVC.

Similarly, the 3GPP system enables the UAV to have a pairing with a networked or cloud UAVC authorized by the USS, by transparently delivering to the USS aviation information that the 3GPP system does not process. The 3GPP system only processes the result of the authorization and decides whether to enable the establishment of connectivity for C2 between a UAV and the specific UAVC (e.g. install traffic filters).The model is based on the following steps:

1. The UAV registers with the 3GPP system using existing procedures and using 3GPP credentials

   The UAV configured and provisioned to perform UUAA (i.e. at a minimum having a UAS ID allocated during a UAV registration with USS) always provides its UAS ID to the 3GPP system when it registers for UAV services.

2. The 3GPP system determines whether to initiate UAV authentication/authorization based on request from UAV, subscription, local policies, and optionally results of previous authentication/authorization

   UUAA by USS/UTM is conditional on the UE having performed successfully a primary 3GPP authentication and with Aerial UE function as part of the subscription

   An UAV is authenticated and authorized by USS/UTM using a UAS ID. The credentials and related authentication method used by the UAV and UTM/USS are outside of the 3GPP scope.

   The UAV may also include an UUAA Aviation Payload containing application layer information that is transparent to the 3GPP System.

   The 3GPP network shall be informed by the USS/UTM of the UAV authentication and authorization result and enforce the result accordingly. Upon successful UAV authentication and authorization by USS/UTM, UAV is authorized to establish limited connectivity to communicate with USS/UTM.

If the result of the UAV authentication and authorization indicated by the USS/UTM is negative, the UAV is informed by the 3GPP system that USS/UTM authentication and authorization has failed.

3. In case of single PDU session/PDN connection for USS and UAVC connectivity:

   - The single PDU session in 5GS can be established without performing any UUAA at PDU session establishment (if UUAA is performed at registration), or UUAA is performed during PDU session establishment if UUAA is not performed at registration

4. For the single PDN connection in EPS, UUAA is performed during PDN connection establishment

   The authorization for connectivity between UAV and UAVC may be performed during PDU session/PDN connection establishment (together with UUAA if UUA is performed), or after the PDU session/PDN connection is established (the details are to be defined during normative work, and may rely on PDU session/PDN connection modification procedures)

5, 6. At any time, the PDU session may be modified (e.g. change of flight authorization, new flight plan, new UAVC) via a modification procedure, which may require further authorization from the USS.

7. In case of separate PDU sessions/PDN connections for USS and UAVC connectivity, the PDU session for USS connectivity in 5GS can be established without performing UUAA at PDU session establishment (if UUAA is performed at registration).

8. UUAA is performed during PDU session establishment in 5GS if UUAA is not performed at registration. For the PDN connection for USS connectivity in EPS, UUAA is performed during PDN connection establishment.

9. When the UAV requires user plane connectivity for C2 the UAV requests a PDU session for UAV operations. The UAV includes in the request the relevant UAV operations information in a transparent container (e.g. UAS ID).

10. The 3GPP system authorizes the PDU session connectivity for UAV operations with a UTM/USS based on the UAS ID.

    To perform authorization for the PDU session/PDN connection for UAV and UAVC connectivity (both in case of single or separate PDU session/PDU connection) the UAV provides to the SMF an Aviation Connectivity Payload containing:

    - the UAS ID

    - an optional Flight Authorization ID that the UAV may have obtained offline by the UAV operator from the USS in order to minimize the amount of information exchanged between the UAV and the USS in the Aviation Connectivity Payload.

    If the UAV has the information on the networked UAV controller or UAVC that connects to the UAV via Internet connectivity (cloud UAVC), the UAV includes also the information for the authorization of UAV and networked UAV controller pairing in the Aviation Connectivity Payload.

    The C2 communication with UAVC should only be allowed (e.g., with setup of appropriate packet filters and access control list) after the pairing authorization is successful.

    Once the USS/UTM has authenticated the UAV and authorized the request for user plane connectivity for C2, this authorization is informed back to the 3GPP system via the UAS-NF

and only then will the 3GPP system allocate the required resources to the UAV and UAVC. The UTM/USS may include in the authorization response information Remote Identification & Tracking Information (RITI) that is transparently provided to the UAV (e.g., a new UAS ID).

After the PDU Session/PDN connection used for C2 communication is successfully established (or modified), the serving 3GPP system should report the device's transport address for C2 communication to the UTM/USS. The UTM/USS should inform the serving 3GPP system of the peer device's transport address for C2 communication.

USS/UTM can provide traffic routing policies for the C2 connectivity which will be used by the 3GPP NFs for data traffic over the allocated user plane resources.

11. When the UAV requires user plane connectivity for C2 and a PDU session or PDN connection already exists, the UAV requests a modification of the PDU session or PDN connection.

12. As step 10.

4.1.2.3 USS and UAS Operator Influencing on UAV cellular connectivity

UAS operator platform or USS are seen by the 3GPP system as application functions (AF) impacting connectivity. The USS and UAS Operator provide connectivity information (e.g. requested QoS, traffic filters, etc.) to the UAV Network Function (NF) in the 3GPP system to configure the connectivity of the UAV to the USS and for C2 via the PDU session/PDN connection. Such traffic influencing function is already part of the SCEF/NEF framework and APIs.

The following capabilities can be requested or influenced by USS or UAS operator:

- For monitoring capabilities:
  - Loss of Connectivity monitoring event may have more stringent latency and time-to-alert requirements, driven by data transmission performance requirement.
  - Roaming status may be enhanced to ensure that UAS connectivity is always handed over to a compliant MNO.
  - Number of UE present may raise an alert when a number of UE with “UAS” APN violates an approved threshold.
  - Downlink data delivery status
- Provisioning capability:
  - Expected UE behavioral information: it seems reasonable for this information to be synchronized with a flight plan available for the USS.
- The Policy capability may be used by USS to restrict available QoS for aerial UEs, to preclude using ‘insecure’ connectivity.
- Network’s External Identifiers may include both Remote ID-compliant UAS identifier as well as USS internal ID used to an associated UAV.

Note: section 6.5 provides a summary of the NEF services/capabilities available for UAS operators.

5. Enabling Remote Identification Via 3GPP Technologies

5.1 Enabling Networked Remote Identification

Networked RID is enabled by providing user plane connectivity between the UAV and the USS. By using a PDN connection/PDU session that supports IP traffic, any UAV-USS traffic can be exchanged. It is expected that configuration of NRID (e.g., frequency, content of messages) may be configured at the application layer between the USS and the UAV.

5.2 Enabling Broadcast Remote Identification

5.2.1 Technologies currently referred to in ASTM F38 and ASD-STAN standards

At present, the following technologies are referred to in ASTM F3411-19 and ASD-STAN Direct Remote ID standard (prEN4709-002) for BRID:

- Bluetooth 4/ Bluetooth 5
- Wi-Fi NAN
- Wi-Fi beacons

These technologies are non-3GPP technologies and are planned to be recognized both by the FAA and EASA as Acceptable Means of Compliance with current regulations.

5.2.2 Using 3GPP Radio Links

3GPP systems have introduced the PC5 interface for Proximity Services (ProSe) since release 15. The functionality of PC5 has been expanded and leveraged in the automotive industry for defining Cellular Vehicle-to-everything (C-V2X) services for vehicular communication services that incorporate all sorts of types of communication, such as V2I (vehicle-to-infrastructure), V2N (vehicle-to-network), V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), V2D (vehicle-to-device) and V2G (vehicle-to-grid).

Most of the requirements related to BRID are expected to be satisfied by the use of PC5 and ProSe services, to be confirmed by the work done in ACJA WT1.

In order to enable the adoption of PC5 for BRID, the following analysis need to be addressed.

5.2.2.1 Protocol Considerations

Broadcast Remote ID assumes that the UAV broadcasts specific messages at regular intervals. The content of such messages may vary depending on the region where the UAS operation occurs. However, independently of the specific BRID protocol considered, such protocols can be “enveloped” into ProSe/PC5 messages. What is required is to:

- identify which ProSe/PC5 messages/services can be re-used,

- map BRID protocol with the ProSe/PC5 messages/services.

The main obstacle in doing so is to identify a body outside 3GPP to perform such task.

5.2.2.2 Security Considerations

The adoption of PC5 cellular connectivity by other verticals (e.g. C-V2X) has considered security to be a must-have building block to ensure robustness of the solution. Given that BRID is meant for identification of UAVs, ensuring strong security is in place for BRID over PC5 is necessary to avoid spoofing and impersonation.

In the example of the C-V2X vertical, a single security solution has been adopted in all geographies and supported by regulators and DoTs, thus ensuring interoperability and a robust infrastructure supporting the vehicular mobility. The UAV ecosystem would benefit from similar advantages if a single solution were defined for security. Moreover, leveraging a single security model for both automotive and UAS would simplify the system and lighten the load on regulators.

Specifically, adopting the C-V2X framework based on IEEE 1609.2 and adapting it to BRID ensures pre-acceptance of a well-known and stable security framework.

5.2.2.3 Spectrum Considerations

In terms of UAV connectivity and types of UAVs, the following scenarios need to be addressed:

- Case 1 - UAV has cellular subscription and operates in MNO space:
  - UAV could operate BRID over PC5 in MNO spectrum
  - MNOs can help manage communications (P2P, Networked, Groupcast, Unicast, etc.)
- Case 2 - UAV does not have cellular subscription and operates in MNO space:
  - UAV does not have cellular subscription and may not have traditional cellular capabilities

Note: in Case 2, there is no cellular connectivity for C2; C2 in this case is typically via dedicated radio links (not PC5) that is outside 3GPP scope

  - UAV cannot operate in MNO spectrum for PC5
- Out of coverage operations must be considered (similar to C-V2X cases), since the UAVs need to send BRID messages even if they operate outside of an MNO coverage.
- interoperability between Cellular UAVs belonging to different MNOs.
- Spectrum allocated to terrestrial PC5 may not be available for airborne use.

Considering the need to minimize the complexity on the BRID receivers, the use of a well known set of frequencies for all UAVs operating in a given airspace is preferrable, thus avoiding receivers having to scan multiple frequencies (e.g. for MNO1, MNO2, and non-cellular UAVs). For this reason, it is recommended that a specific spectrum is allocated for PC5 for BRID.

5.2.2.4 Interface with stakeholders

One aspect which needs to be considered as well is the capability for the ProSe/PC5 messages to be received directly by existing mobile devices within the broadcasting range.

6. Use of Cellular Connection for Remote ID and C2

This section aims at covering the use of Uu (UAV to cellular network) connectivity for C2.

This will not cover KPIs, unless Work Task #3 identifies some missing KPIs that need to be brought to 3GPP.

6.1 Scenarios for Cellular Connectivity

This section highlights the impact of connectivity scenarios with respect to the ability to provide RID services (i.e., what is feasible and what is not), and does not recommend what should be made available in the various scenarios.

Table 2.1-1: Cellular connectivity availability scenarios for Remote Identification

	Cellular Connectivity available at			
	Take off + In flight	Take Off / Lost in flight	Not at takeoff / In flight	Not at takeoff / not in flight
Networked C2 connectivity only scenario	Regular case	UAV behavior out of scope of 3GPP *(must assume application layer safety measures, e.g. land safely, continue flight plan, etc.)*	Not Allowed *(no control on UAV at takeoff)*	Not Allowed *(no UAV control at all, this must be a fully automated flight without connectivity - not allowed yet?)*
Remote Identification (both BRID and NRID)	Regular case, both BRID and NRID available	NRID used only when cellular connectivity is available, BRID available all the time	Must rely on offline/previous configuration for BRID, NRID used only when cellular connectivity is available	Must rely on offline/previous configuration for BRID. NRID never used
Only NRID	Regular case	No Remote Identification possible, which would not satisfy regulations that require NRID to enable flight.		

6.2 Cellular Connectivity for C2, UAV-USS Communications, and Networked Remote ID

C2 between a UAV and a remote UAVC is supported by the cellular system via PDU Sessions/PDN Connections to an appropriate Data Network, whose APN/DNN is configured by the MNO.

Network Remote ID is similarly supported via PDU Sessions/PDN Connections to an appropriate Data Network, whose APN/DNN is configured by the MNO and must allow connectivity with the USS.

If network slicing is used in 5GS, with specific network slices deployed for UAS services, the network slice identifiers need to be provisioned to the UAV and the UAV must be provisioned with information regarding the use of slices and related DNNs for UAS services.

It is assumed that the MNO network support either single PDU session/PDN connection for USS and C2 connectivity, and separate PDU sessions/PDN connections for USS and C2 connectivity are supported. The mechanism that may be used is up to deployment.

The USS/UTM is not assumed to have knowledge of PDU sessions or PDN connections: the USS/UTM authorizes connectivity requests sent from the 3GPP system for a UAV or UAV controller, can revoke such authorization, and can provide information to control such connectivity (e.g. ACL, QoS information, etc.).

7. Location and Flight Tracking

This section addresses the services provided to a USS by MNOs for location and flight tracking and does not relate directly to Remote Identification.

3GPP networks provides the functionality of UAV tracking as a service to USSs and UTM via service exposure framework. A USS can use the service exposure Web APIs to access the UAV tracking services provided by a 3GPP network.

The following assumptions are at the basis of such service:

- A UAV has been registered to the USS with the support of the 3GPP system, and during such procedure the 3GPP UAV ID is provided to the USS
- When available, the USS triggers the UAS tracking by an MNO providing the 3GPP UAV ID(s) of the UAV(s) to be tracked

Three UAV tracking modes are supported:

- UAV location reporting mode:

  In this mode, the USS that wants to receive the UAV location subscribes to the MNO service providing the target 3GPP UAV ID, and optionally providing the required location accuracy and whether it's for immediate reporting (e.g. one time reporting) or deferred reporting (e.g. periodic reporting).

- UAV presence monitoring mode:

  In this mode, the USS subscribes for event reporting of UAV moving in or out a geographic area (e.g. longitude/latitude, zip code, etc.) by providing the target 3GPP UAV ID and information on a geographic area. Mapping of the geographic area onto 3GPP location tracking mechanisms is performed by the 3GPP system. The USS receives event notifications when the UAV enters/exits the indicated geographic area. The USS may also provide policies to the 3GPP system indicating actions to be taken upon even notification (e.g. remove C2 connectivity for the UAV), depending on USS policies.

- Unknown UAV tracking mode:

  In Unknown UAV tracking mode, the USS (or a public safety function) requests to an MNO a list of the UAVs in a specific geographic area and that are served by the MNO. The 3GPP system identifies all UAVs served by the MNO in the provided area and reports to the USS the corresponding list. The 3GPP system will provide to the subscribing function the list of 3GPP UAV IDs and UAS IDs corresponding to the identified UAVs.

8. Security Aspects

8.1 Overall security architecture of the UAS-USS model

The use of Remote Identification for UAV tracking and identification requires mechanisms to ensure an acceptable level of security. Though regulatory bodies are still discussing, and sometimes only marginally, security issues of Remote Identification, the experience of the automotive industry and of V2X has demonstrated how a solid security solution at the application layer is essential to the success of this type of solutions. 3GPP is not the correct forum to define such security, since such security aspects span to architectural elements and deployments beyond the scope of 3GPP (e.g., the USS).

This section describes a method of applying the transportation industry's IEEE 1609.2 cryptographic credential and security services, already adopted by V2X, to ASTM 3411-19 *Standard Specification for Remote ID and Tracking*. The annex provides a concept definition and security model for implementing the IEEE 1609.2 security standard as a means of securing UAS identity and tracking communications. It meets basic operating concepts described in the FAA's proposed Drone ID and Tracking NPRM, apply the 1609.2 security model and allow the security services of 1609.2 to function within the constraints of ASTM Remote Identification.

Unmanned Aerial Systems (UAS) require lightweight, strong cryptographic certificates in order to apply authentication and integrity controls to identity and tracking-related information, especially in network-disconnected paradigms. Network-disconnected operation is characterized a receiver of the UAS broadcast having degraded or no cellular or other IP connectivity, no DNS services and therefore no access to application or network authentication services. When network connectivity is available, enhanced support to 1609.2 becomes available.

The transportation industry's Wireless Access in Vehicular Environments (WAVE) protocol is defined in the IEEE 1609-series of standards. While the 1609.2 security services were engineered for V2X communications in the 5.9GHz licensed band, they operate above the radio access layers and are suitable for use in any mobile IoT, application or network security communications. Given the small size of the 1609.2 certificate, it can be used effectively within the beacon frame constraints of Wi-Fi and Bluetooth. Well-structured interfaces and primitives allow the security model to be enforced in an unlimited number of application paradigms, and a variety of existing infrastructure and provisioning services are available today to deploy 1609.2 communications security.

8.2 Security model for UAS authentication/authorization to USS via the 3GPP MNO

An UAV may be authenticated and authorized by USS with the optional support of the 3GPP system before connectivity for UAS services (e.g., UAS-USS connectivity for NRID) is enabled. The existing 3GPP authentication and authorization framework is leveraged as much as possible to minimize the impact on 5GS and EPS system protocols

When the 3GPP system supports the UAV authorization by the USS, an interface based on Web API service exposure is assumed between the MNO and the USS, which does not imply a strict connection between the MNO and the USS and is based on 3GPP external service exposure framework.

A UAV provides a UAS ID to the 3GPP system. The 3GPP system determines whether to initiate UAV authentication/authorization based on the request from UAV, the UAV subscription being a UE aerial subscription, local policies, results of previous authentication/authorization, and the UAV having provided the UAS ID. The USS can revoke such UAV authorization.

NOTE: the UAS ID may be an identified as the “Session ID” identified e.g., by FAA regulations.

UAV authentication and authorization by USS is conditional on the UE having performed successfully a primary 3GPP authentication and with Aerial UE function as part of the subscription.

An UAV is authenticated and authorized by USS using a UAS ID. The credentials and related authentication method used by the UAV and USS are defined in this document.

The 3GPP network shall be informed of the UAV authentication and authorization result and enforce the result accordingly (e.g. enable or deny aerial services). Upon successful UAV authentication and authorization by USS, UAV is authorized to establish limited connectivity to communicate with USS, but connectivity for C2 cannot be established until explicitly authorized by the USS.

A UAV request for user plane connectivity to the 3GPP system for UAV operations (i.e., C2 between a UAV and a networked UAV controller and/or flight authorization request) may also require additional authorization by the USS.

8.3 C2 privacy and integrity

Two cases are considered in the scope of the 3GPP ecosystem:

- the UAVC is a 3GPP UE, i.e. is a cellular device. In this case, C2 connectivity is transported over two Uu connections, one for the UAV and one for the UAVC, plus potentially an inter-MNO connection if the UAV and the UAVC are served by two different MNOs.
- the UAVC is a cloud device located in the internet. In this case, C2 connectivity is transported over Uu connectivity and over Internet links

C2 connectivity is secured over Uu using cellular security, which provides encryption and integrity protection between the mobile device and the MNO core network. No additional mechanisms specific to UAVs are required to protect C2 connectivity over Uu.

However, if C2 connectivity traverses open Internet connectivity, it is expected that application-level mechanisms will be in place between the UAV and the UAVC to protect C2 connectivity over exposed Internet links.

8.4 Remote Identification Security

8.4.1 Objectives of Security Model for Remote Identification

ASTM has touched on some security aspects of Remote Identification in the standard used as basis for the FAA NPRM. In their NPRM on Remote Identification, the FAA has briefly touched on security aspects but has not defined any solutions.

In ASTM discussion, and in IETF discussion, it is becoming clear that in order to have successful deployments of Remote Identification, security solutions are required for both Broadcast Remote Identification and Networked Remote Identification. Networked Remote Identification can leverage the cellular connectivity security that protects the traffic exchanged over the air, in addition to any potential application layer security.

The following objectives are derived directly from the FAA NPRM, the ASTM Remote Identification standard, the requirements and architectural assumptions of the IETF DRIP work:

- OBJECTIVE 1: Enable broadcast receivers to trust the authenticity and integrity of broadcasts when disconnected from IP/cellular services
- OBJECTIVE 2: Minimize cryptographic security overhead in order to fit cryptographic security primitives into the frame size and field constraints of Bluetooth and Wi-Fi beacons
- OBJECTIVE 3: Support privacy-preserving, secure broadcast wherein USS identity information is not linkable to the operator and is only accessible to authorized parties such as regulators and law enforcement
- OBJECTIVE 4: Support network-disconnected as well networked ID & Tracking operations. Scenarios include UAS and Receiver both connected to network, UAS and Receiver both disconnected from the network, UAS connected to network while Receiver disconnected from network, and UAS disconnected from network while Receiver is connected to the network
- OBJECTIVE 5: Support but don't restrict USS/UTM network authentication methods such that various commercial, industry-standard network authentication methods are usable to USS operators. TLS using IEEE 1609.2 (ISO 21177), X.509 certificates, OAUTH, cellular CN services, Host Identity Protocol (HIP) and many others may be used in network security and authentication. Different USS/UTM systems may support different methods based on cost, commercial viability as well as functional needs and differentiation in service offerings.
- OBJECTIVE 6. Minimize cost and time to deploy
- OBJECTIVE 7. Support a robust security model that integrates well into supply chain security best practices in the enrolment and bootstrap of UAS platforms.

A 1609.2 implicit certificate is approximately 100 Bytes, small enough to be transmitted in an ASTM Remote Identification defined message frame [OBJECTIVE 1, OBJECTIVE 2].

IEEE 1609.2 allows *Pseudonym certificates* that contain no long-term, static identity information linkable to the certificate owner, are intended to have very short lifetimes and only be used for short durations to help preclude tracking and correlation threats [OBJECTIVE 1, OBJECTIVE 3]. It also allows *Identity certificates* which contain static, identifying information specific to the certificate owner, and may be used for long periods of time [OBJECTIVE 1].

8.4.2 Prerequisites to 1609.2-Secured UAS ID & Tracking

Prerequisites include:

- A Certificate Authority trust chain is allocated to the broadcast recipient. This is a signed structure indicating one or more Certificate Authorities and their roots of trust. This structure may be published electronically and downloadable. UAS devices that need to receive and process UAS broadcasts from other UASs must be similarly provisioned.

- The UAS is provisioned a 1609.2 Enrolment certificate. The UAS will use this certificate for requesting flight-usable Authorization certificates from an approved certificate provider (Certificate management processes are defined in **Error! Reference source not found.**).
- The UAS is issued an Authorization certificate it will use to sign its broadcasts. This certificate is defined as an IEEE 1609.2 Identity Certificate

  NOTE: the certificate type must be 'Implicit' to ensure the compactness of the certificate and its ability to be broadcast within the message size limitations identified for UAS)

- The broadcast receiver has obtained the UAS signing certificate (broadcasted at intervals) such that it can verify signed messages broadcast from the UAS

8.4.3 Relationship Between UAS Identity, Certificate and 1609.2 Authentication

ASTM Remote Identification and the proposed Federal Aviation Regulations intend to support three identification methods: UAS Serial Number per the ANSI/ CTA-2063-A Serial Number format, Civil Aviation Authority (CAA) issued Registration ID, and UTM-assigned Identifier in the form of a 128-bit UUID (16 Bytes).

The use of IEE 1609.2 supports all three formats:

- Serial Number Identification and Authentication: the UAS serial number populates the certificate_id field within the 1609.2 certificate. The UAS may authenticate the messages using the private key pairwise with the public key associated with this certificate. Only the UAS maintains a copy of this private key. The UAS certificate size when embedding a UAS Serial Number is 86 Bytes.
- CAA-Issued Registration Identifier and Authentication: the CAA-issued identifier populates the certificate_id field within the 1609.2 certificate, and the total UAS certificate size when embedding a CAA-Issued Registration ID is up to 90 Bytes.
- USS/UTM-Issued UUID and Authentication: A UAS may be identified using a time-limited UUID similar to a network session ID, intended to be short-lived to reduce tracking related privacy threats to UAS operators. In this case in order to cryptographically authenticate the UUID, either the the UUID is embedded in the UAS certificate, or the UUID is defined as the least significant 16 Bytes of the SHA-256 hash of the UAS certificate. Either option may be performed depending on the USS and certificate services business model. The latter option is simpler and negates the need to manage both a UUID and a certificate hash to link the UUID to the certificate. In the first option the UAS certificate size is 86 Bytes, whereas in the second option it is 72 Bytes. The USS/UTM computes the UUID by performing an IEEE 1609.2 HashedId16 of the UAS certificate, where HashedId16 is the least 16 significant bytes of the certificate's SHA-256 hash.

A fourth option is possible for the UAS identification when using IEEE 1609.2, i.e., identification of the UAS using a cryptographic hash of its certificate.

8.4.4 Certificate Management Services

Existing 1609.2-supporting PKI definitions, client interfaces and services are available today for use in Remote Identification.

The PKI is the source of 1609.2 credential-based trust for UAS operating in the National Airspace System. It consists of the following nodes:

- Root CA: the root of trust, a self-signed or Elector-signed credential used to issue Intermediate CA, Enrollment CA and other CA credentials within the PKI.
- Enrollment CA: issues Enrollment Credentials to UAS communications module in the manufacturing environment. Though this is traditionally not done yet, it is an essential component of the solution, and a complete security solution shall define what piece of hardware in the UAV stores the Enrollment Credentials.
- Intermediate CA: issues other Intermediate CAs, Misbehaviour Authorities, Enrollment Authorities and Authorization Authorities.
- Authorization CA: signs and issues Authorization Certificates for UAS. Authorization certificates may be of type Identity (uses static identifiers) or of type Pseudonym (short-term certificates with no publicly linking identifiers linking operator to the UAS). The UAS does not interact directly with the ACA but most go through a Registration Authority.
- Registration Authority (RA): provides the external interface through which a UAS obtains Authorization certificates from the Authorization CA. The RA may be run by a USS provider, or the USS may have direct, contracted services from a RA. The UAS may connect to the RA directly or via the USS.
- Misbehavior Authority (MA): is the PKI entity through which the FAA may revoke a UAS enrollment from its trust relationship in the National Airspace System (NAS). The FAA may indicate (directly, or via a USS) that a UAS with a specific serial number, Enrollment certificate or Authorization certificate needs to be revoked. The MA coordinates the blacklisting of the Enrollment credential (such that it may obtain no more Authorization certificates) and the addition of the UAS to a published Certificate Revocation list (CRL). The MA (or the Enrollment CA, depending on the implementation) will expose an interface to Law Enforcement that allows the discovery of the UAS owner/operator associated with a given certificate (as obtained by a misbehaving UAS broadcasting its certificate-signed ID/Tracking data).

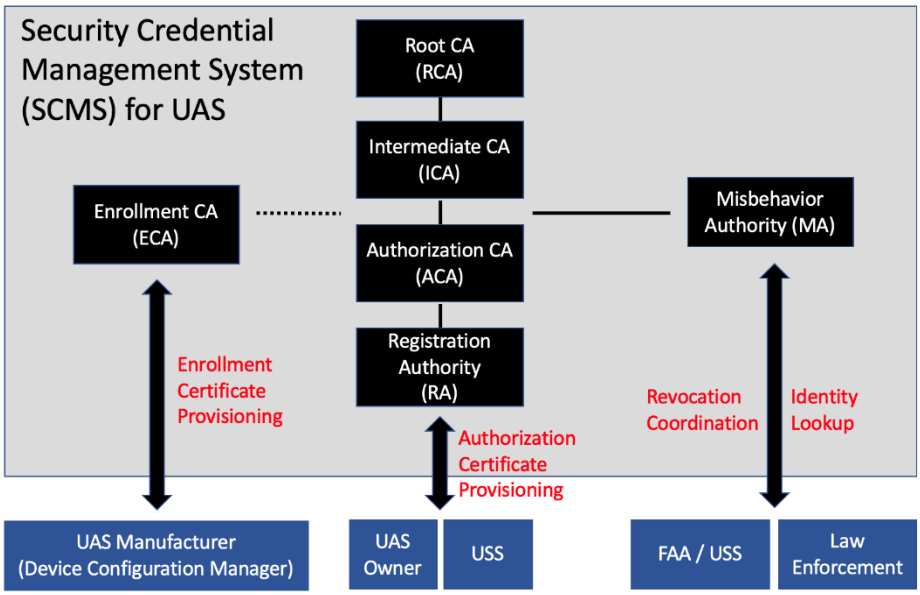

Figure 8.4.4-1: 1609.2 Public Key Infrastructure High-Level Architecture

The following diagram describes the supply chain and provisioning considerations for the use of 1609.2 certificates.

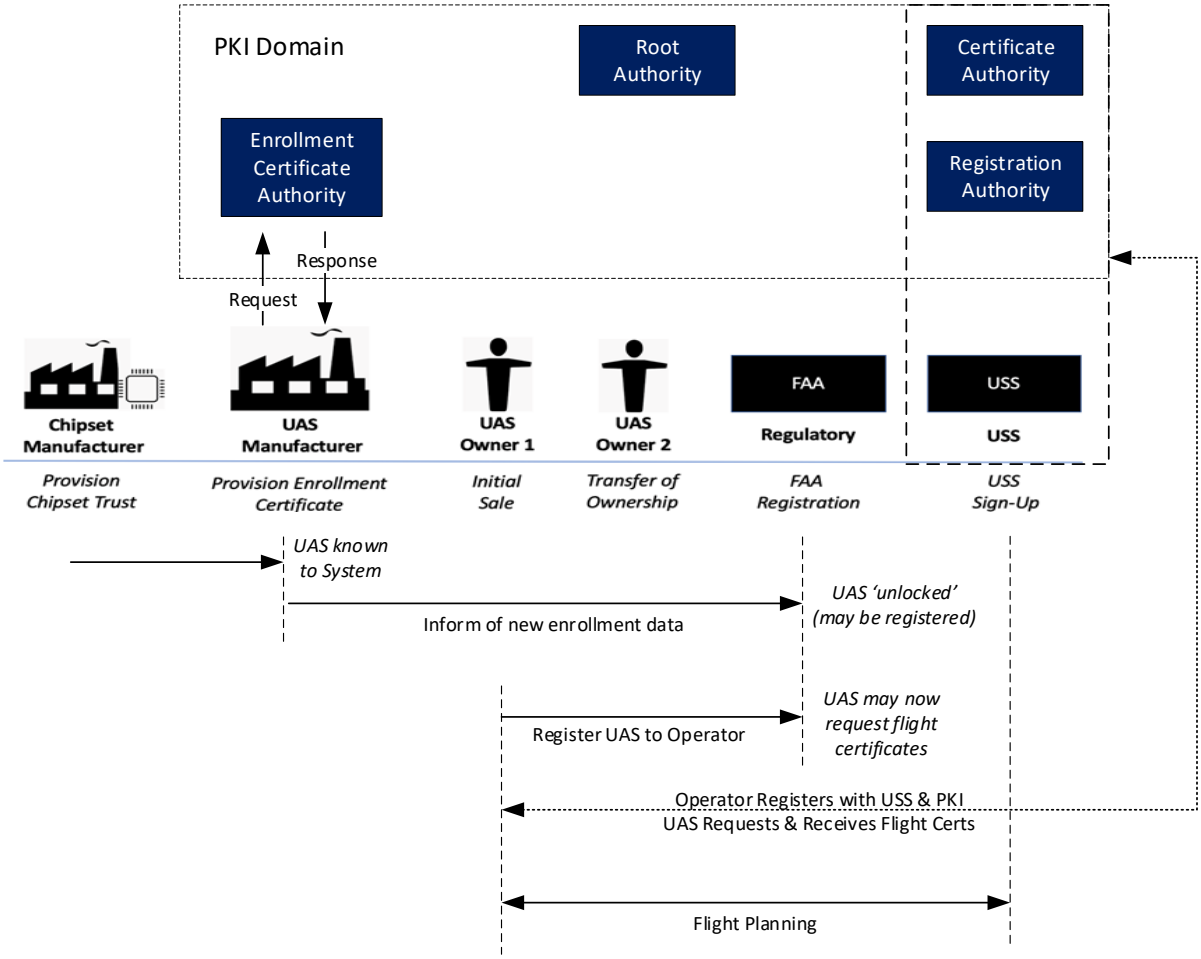

Figure 8.4.4-2: 1609.2 Certificate Logical Flow.

The following table depicts the security information relevant to the application of IEEE 1609.2 certificate to UAS.

Table 8.4.4-1: security information relevant to the application of IEEE 1609.2 certificate to UAS.(Source 3GPP)

Parameter	Description
UAS Chipset Root of Trust (Canonical Identifier)	Installed in hardware security module during manufacturing Used in the manufacturing supply chain to validate authenticity of the module May be used as a PKI Enrollment trust mechanism in lieu of enrollment being performed in a well-secured environment. If so, the device would sign an enrollment request with the PKI and then receive its Enrollment certificate (later used to request operational 'Authorization Certificates')

	While the Civil Aviation Authority (CAA) does not need to be aware of the UAS chipset Root of Trust, the CAA may request manufacturer support to accesses this root of trust during forensic or accident investigations
UAS Serial Number	The unique serial number (identity) of the UAS, embedded in the UAS Enrollment credential which is NOT used to sign ID/tracking messages If privacy is not required, the UAS Serial Number may also be embedded in the UAS Authorization Certificate If privacy is required, the UAS Serial Number may be omitted from the UAS Authorization Certificate, and the Authorization Certificate may be of type 'Pseudonym'
UAS Enrollment Seed Key	A public and private keypair generated on the UAS hardware security module or within the manufacturer's secure server and then injected into the UAS in the manufacturing environment The Seed Private Key is used by the UAS to digitally sign an Enrollment Certificate request generated by the HSM and sent to the PKI The Seed Public Key is used by the Enrollment CA to verify the signature on the enrollment certificate request, and is embedded into the final Enrollment Certificate
UAS Enrollment Certificate	The unique identity for the secure communications module embedded in the UAS. Embeds the seed public key and UAS serial number and to which the communications module is bound. Obtained by the UAS via an Enrollment certificate request/response exchange with the PKI. Once the UAS has received an enrollment response message from the PKI, the UAS Enrollment Certificate and associated private key are stored in the communications module HSM. The UAS manufacturer associates this certificate to the Chipset Root of Trust Once the UAS is sold to an operator, the UAS Enrollment certificate's private key is used to digitally sign requests (to the PKI or USS proxy) for Authorization Certificates The UAS manufacturer reports to the FAA the UAS Enrollment certificate and the UAS Serial number, or the FAA stores or has access to via an interface with the PKI or USS.
UAS Authorization Certificates (UAV Unique Identity)	Obtained by the UAS operator (or the USS, if by proxy) from the PKI via an authorization certificate request and response with the PKI. Authorization certificate requests are signed by the UAS using the UAS Enrollment Certificate Used to digitally sign (authenticate) Broadcast ID/Tracking messages May be used to network-authenticate the UAS to a USS provider (depending on the USS-specific interface). If this is the case, the USS may operate its own PKI Registration Authority. May contain permanent serial number information OR it may be pseudonymous, depending on operator type and preferences

8.4.5 Networked RID privacy and integrity

UAS may use X.509 or IEEE 1609.2 digital certificates to securely end-to-end connect the UAS with the USS. In order to enhance privacy, the UAS may perform an anonymous TLS handshake followed by an in-tunnel authentication of the UAS.

NOTE: a mutual TLS handshake could be also used, since both the UAS and the USS server have a certificate installed.

TLS will cryptographically protect the privacy and integrity of the communications between the UAS and USS.

8.4.6 Broadcast RID privacy and integrity

A broadcast receiver obtains a UAS Authorization certificate in order to verify messages originating from the UAS in the following way:

- when network-connected, a broadcast receiver may also query an authentication service to either obtain a copy of a UAS authorization certificate based on the information the receiver detected from a signed broadcast, or send the authentication material service for a proxy-verification of the signature, as described in ASTM Remote Identification. In a flight where the UAS is transitioning in and out of network connectivity, both options may be necessary. In some instances of network connectivity, broadcast receivers may elect to cross-correlate authenticated UAS Broadcasts with authentication from the authentication service.
- when disconnected from the network, the message receiver has no access to networking infrastructure or authentication services.
    - The UAS periodically broadcasts (with a configurable periodicity) its own authorization certificate using the Peer-to-Peer certificate distribution [P2PCD] protocol in IEEE 1609.2, designed for use in disconnected environments when a message recipient is unable to verify a message to a complete cryptographic trust chain due to lack of a certificate. UAS uses this technique to make their authorization certificates known. CA certificates are assumed to be pre-installed in broadcast recipients and made updatable via ID/Tracking PKI certificate services.
    - Message receivers extract the UAS authorization certificate from the UAS broadcast, verify the certificate based on its public key reconstruction value and known CA certificate, and associate the UAS authorization certificate to the reconstructed public key from the certificate.

Given the low flight speeds anticipated in most small UAS, the recommended certificate broadcast rate will likely range between 5 and 10 seconds. Thus, any messages detected by the broadcast are guaranteed to be verifiable within a 5 to 10 seconds interval of time. All subsequent messages transmitted by the UAS will be immediately verifiable with the cached certificate.

The solution must uniquely identify and authenticate the UAS identity, with an option for privacy. Privacy is needed in the form of public unlinkability, such that the general public cannot identify or easily track the operator but law enforcement and the FAA can. Unlinkability, if needed, can be obtained by using very short-lived certificates and otherwise refraining from using long-term identities (in the form of digital certificates).

If either the UAS or its control station is disconnected from the network, law enforcement and other observers must still be able to trust the UAS identity. To meet this need, BRID will leverage IEEE 1609.2 and its provision for:

- A lightweight cryptographic certificate format using strong Elliptic Curve Cryptography (ECC). The 1609.2 certificate comes in an *explicit* format in which the end entity's full public key is contained in the certificate signed by the Certificate Authority (CA). It also comes in an *implicit* format "that allows the associated public key to be reconstructed from a reconstruction value and the certificate authority's public key rather than directly providing the associated public key." Implicit certificates are based on the Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)
- A security framework and set of primitives that enable the certificate to be used for to meet a variety of communications security objectives beyond simple identification and authentication of the message or its sender. These include optional message consistency checks, relevance checks and a variety of other 1609.2 security profile settings that can be tuned to the needs of a given application.

BRID messages will be digitally signed with the 1609.2 private key such that message recipients can detect integrity failures and spoofing and ensure data origin. A UAS identity will be indicated via the 1609.2 public key certificate corresponding to the private signing key. The UAS will periodically broadcast this certificate along with the signed BRID data. The certificate's public key will be used by message recipients to cryptographically verify the UAS' message.

The private key is stored only within the UAS. It must be issued securely provisioned to the UAS, stored in secure hardware, and never exported or shared.

The BRID messages are defined in ASTM F3411-19. The detailed use of 1609.2 to secure the broadcasts is as follows:

1. To prevent spoofing of ID/Tracking transmissions from the UAS, the UAS will digitally sign the ID/Tracking Message ("broadcast") using the private key corresponding to the IEEE 1609.2 public key or reconstruction value embedded in its 1609.2 Authorization Certificate ("flight certificate")
2. The UAS will periodically send an ASTM 3411-19 Authentication message containing the full certificate it is using to authenticate broadcasts.
    a. In cases where privacy of the UAS operation is not needed, this certificate will be an IEEE 1609.2 Identity Certificate
3. The UAS will append the signed message with either its signing certificate (containing the corresponding public key) or the hash of its signing certificate
4. Receivers of the message will perform a signature verification of the message using the Authorization certificate public key and/or its reconstruction value. If the message verifies, it is accepted as trusted and valid. If the message verification fails, the message will be flagged and discarded.

9. Appendix: 3GPP System Architecture

9.1 EPS System Architecture

The Evolved Packet System Architecture [5] has three components:

- The User Equipment (UE): the UE is composed of two main modules
    - The Mobile Equipment (ME) which handles the communication functions and terminates the data streams.
    - The Universal Integrated Circuit Card (UICC), also known as the SIM card, which runs the Universal Subscriber Identity Module (USIM) application and stores user-specific data (e.g., information about the home network identity, security keys, etc.).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN): handles the radio communications between the mobile and the EPC. It is composed by a series of eNodeBs (eNBs), which are base stations that, when serving the UE, controls the UE in one or more cells. The eNB sends and receives radio transmissions to all the UEs using the LTE air interface, and the access stratum operation of all the UEs it is serving via access stratum signaling messages (e.g., handover commands).
- The Evolved Packet Core (EPC), which communicates with packet data networks in the outside world such as the internet, private corporate networks, or dedicated service networks.

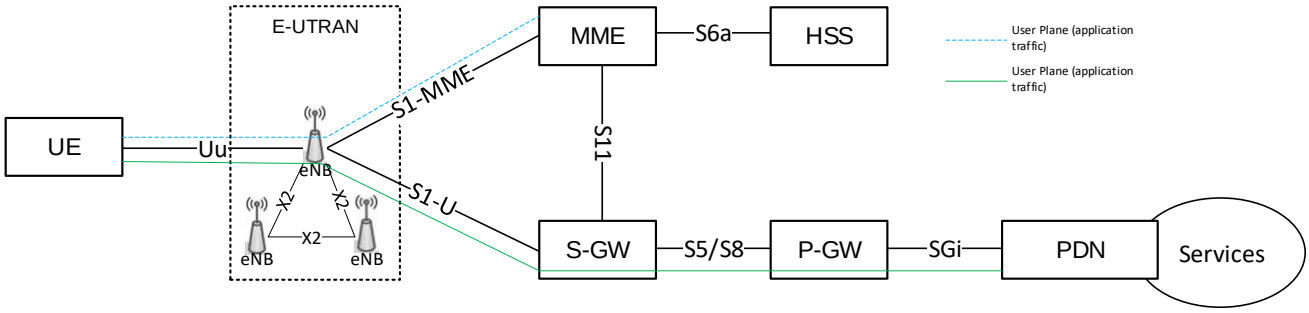

Figure 9.1-1: EPS Architecture. (Source 3GPP)

The EPC is composed of the following functions:

- The mobility management entity (MME) controls the Non-Access Stratum (NAS) operation of the mobile via NAS signaling messages, handling mobility management and session management procedures.
- The Home Subscriber Server (HSS) is a central database that contains information about all the network operator's subscribers.
- The Packet Data Network (PDN) Gateway (P-GW) communicates with the external packet data networks (PDNs) using the SGi interface. Each packet data network is identified by an access point name (APN), which is used in session management signaling to establish connectivity to the PDN corresponding to the APN.

- The serving gateway (S-GW) acts as a router, forwards data between the base station and the PDN gateway, and acts as mobility anchor to support mobility within the mobile network.
- The Policy Control and Charging Rules Function (PCRF) is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW.

9.2 5GS System Architecture

The 5G System (5GS) architecture ([6], [7]) leverages virtualization and cloud computing by implementing a service-based architecture, providing a distributed set of functionalities. In addition, the 5GS implements user plane function (UPF) to decouple packet gateway control and user plane functions, and access and mobility management function (AMF) to segregate session management functions from connection and mobility management tasks.

The 5G System Architecture has three components:

- The User Equipment (UE): the UE is composed of two main modules
    - The Mobile Equipment (ME) which handles the communication functions and terminates the data streams;
    - The Universal Integrated Circuit Card (UICC), also known as the SIM card, which runs the Universal Subscriber Identity Module (USIM) application and stores user-specific data (e.g. information about the home network identity, security keys, etc.).
- The Next Generation Radio Access Network (NG-RAN): handles the radio communications between the mobile and the 5GC. It is composed by a series of gNodeBs (gNBs), which are base stations that, when serving the UE, controls the UE in one or more cells. The gNB sends and receives radio transmissions to all the UEs using the NR air interface, and the access stratum operation of all the UEs it is serving via access stratum signaling messages (e.g. handover commands).
- The 5G Core Network (5GC), which communicates with packet data networks in the outside world such as the internet, private corporate networks or dedicated service networks.

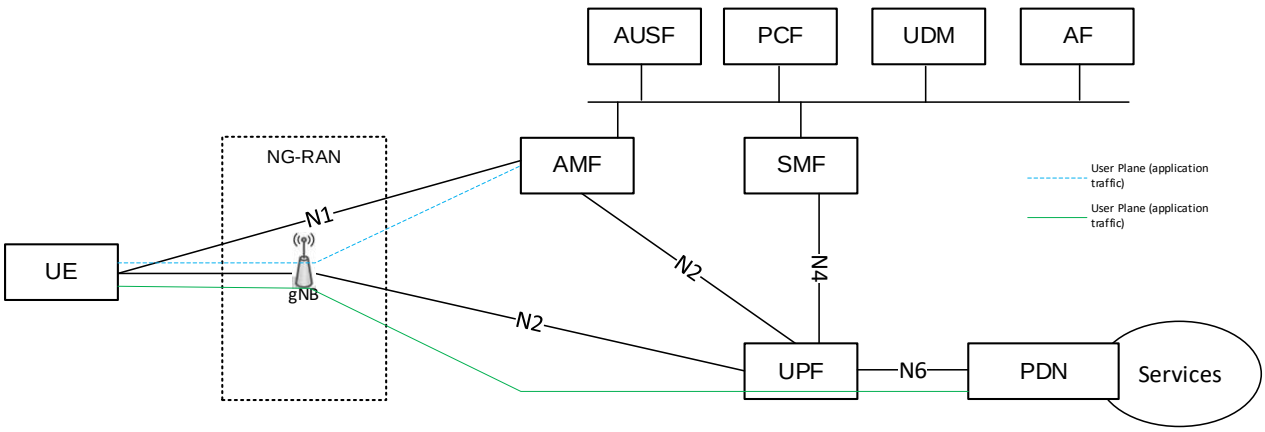

Figure 9.2-1: 5GS Architecture. (Source 3GPP)

- The 5GC is composed of the following functions:
- The Access control and Mobility Management Function (AMF) controls the Non-Access Stratum (NAS) operation of the mobile via NAS signaling messages, handling mobility management
- The Session Management Function (SMF) controls session management procedures and controls establishment of user plane resources in NG-RAN and User Plane Function (UPF).
- The Unified Data Management (UDM) is a central database that contains information about all the network operator's subscribers. The UDM generates security credentials, provides user identification, access authorization, and subscription management,
- The Authentication Server Function (AUSF) a performs the authentication function of EPS HSS.
- The Policy Control Function (PCF) contains UE specific policy rules for control plane functions, derived by subscription information or provided by an external Application Function (AF).
- The User Plane Function (UPF) performs packet routing and forwarding, packet inspection, and QoS handling.

9.3 Registration and Connectivity Services

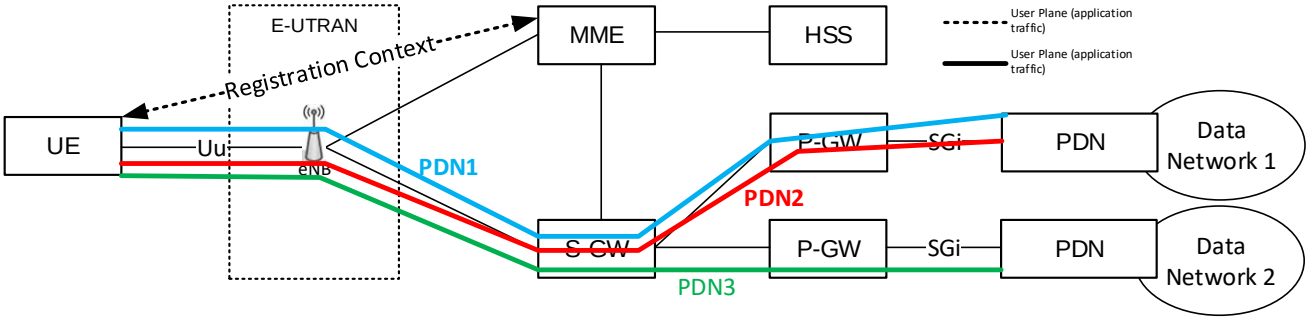

Figure 9.3-1: Registration and connectivity in EPS.

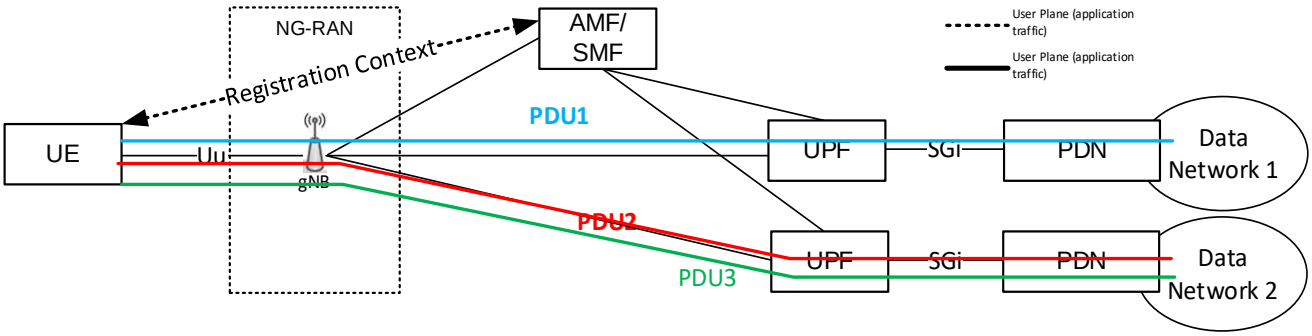

Figure 1.3-2: Registration and connectivity in 5GS.

A UE will perform a registration with the EPS/5GS when entering the system: the registration uses the UE subscription with the MNO to authenticate the credential in the USIM, and to create a mobility management context for the UE as part of the registration context. Part of the registration may include the validity of the UE hardware based on the IMEI assigned to the UE communication module.

When the UE requires connectivity, the UE establishes one or more PDN Connections in EPS (each to a specific Access Point Name identifying a specific data network), or PDU Sessions (each to a specific Data Network Name identifying a specific data network) in 5GS. The UE may support one or more concurrent PDN Connections/PDU sessions anchored at different gateways, depending on the data network. Typically, the UE is configured with a mapping between specific applications and the APN/DNN to be used for transporting user plane data of such applications.

9.4 Exposure of Network Functions

The Service Capability Exposure Function (SCEF) in EPC is a functional element, which provides a means to securely expose the services and capabilities provided by 3GPP network interfaces. The SCEF provides access to network capabilities through homogenous application programming interfaces. The SCEF protects the other PLMN entities (e.g., HSS, MME) and provides a single point of contact for Application Server (AS) trying to access various capabilities exposed by the network. The SCEF also supports mapping between information exchanged with AS (e.g., geographical identifiers) and information exchanged with internal PLMN functions (e.g., cell-Id, eNB-Id, TAI, MBMS SAI etc.). Similarly, the Network Exposure Function (NEF) supports external exposure of capabilities of network functions in 5GC. Figure 6.4-1 below shows a high-level architecture of network/service capability exposure supported by the 3GPP network for EPC and 5GC. Network capability exposure to external Application Function (AF) or Application Server (AS) is possible for both Roaming and non-Roaming scenarios with support for interworking between 5GC and EPC.

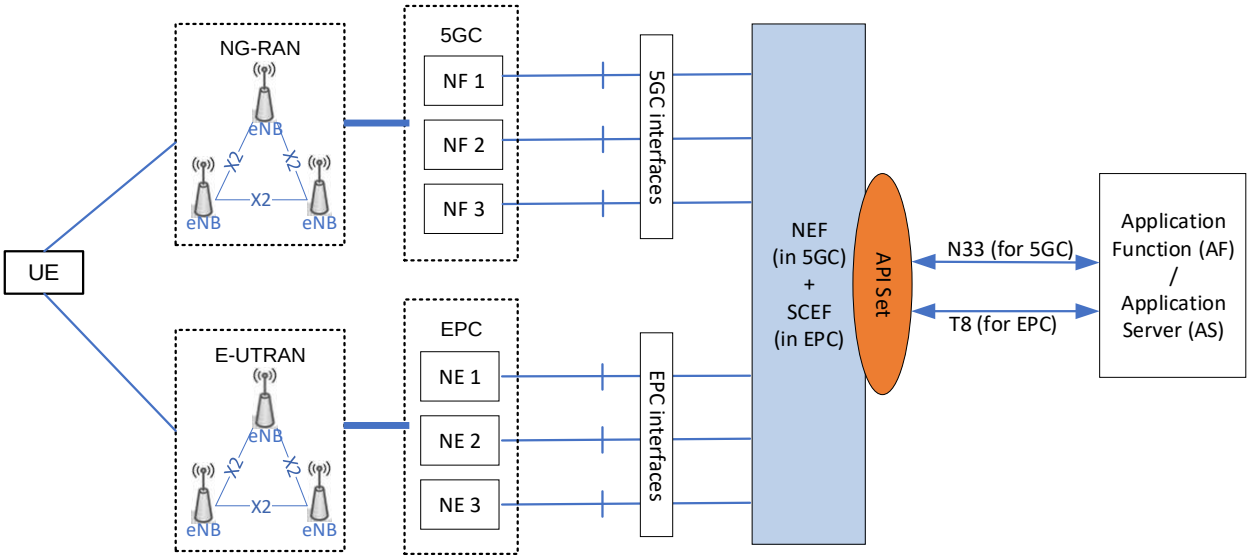

Figure 9.4-1: Network/Service Capability Exposure Architecture for EPC and 5GC (Source 3GPP)

External exposure can be categorized as Monitoring capability, Provisioning capability, Policy/Charging capability and Analytics reporting capability:

- The Monitoring capability is for monitoring of specific event for UE in 3GPP System and making such monitoring events information available for external exposure via the NEF (for

5GS) or SCEF (for EPS). It is comprised of means that allow NFs in EPS/5GS for configuring the specific events, the event detection, and the event reporting to the requested party. The monitoring events supported by the 3GPP system include:

- Loss of Connectivity
- UE reachability
- Location Reporting
- Change of SUPI-PEI association
- Roaming status
- Communication failure
- Availability after Downlink Data Notification failure
- PDU Session Status
- Number of UEs present in a geographical area
- CN Type change
- Downlink data delivery status
- UE reachability for SMS delivery

- The Provisioning capability is for allowing external party to provision of information which can be used for the UE in 3GPP System. Provisioning capability allows an external party to provision the following information:
    - The expected UE behavioral information, which consists of information on expected UE movement and communication characteristics
    - The 5G VN group information, which consists of information on 5G VN group
    - The service specific information, which consists of information to support the specific service in 5G system
- The Policy/Charging capability is for handling QoS and charging policy for the UE based on the request from external party. The AF may request that a data session to a UE is set up with a specific QoS (e.g., low latency or jitter) and priority handling. The AF can request the network to provide QoS for the AF session based on the service requirements with the help of a QoS reference parameter which refers to pre-defined QoS information.
- The Analytics reporting capability is for allowing an external party to fetch or subscribe/unsubscribe to analytics information generated by 3GPP System. This applies only for 5G. An AF may request for being notified about the network status, in a specific geographical area or for a specific UE. After receiving the request for network status notification from the AF, the NEF retrieves user data congestion analytics information from NWDAF, as defined in TS 23.288 [9].

UE identification in the 3GPP system is based on the following:

- Each subscriber in the 5G System shall be allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system.
- The 5G System supports identification of subscriptions independently of identification of the user equipment. Each UE accessing the 5G System shall be assigned a Permanent Equipment Identifier (PEI).

- Each subscriber may have one or several External Identifier(s) that are stored in the HSS/UDM. External Identifier shall be globally unique. Generic Public Subscription Identifier (GPSI) is needed for addressing a 3GPP subscription in different data networks outside of the 3GPP system.
    - The 3GPP system stores within the subscription data the association between the GPSI and the corresponding SUPI.
    - GPSIs are public identifiers used both inside and outside of the 3GPP system. The GPSI is either an MSISDN or an External Identifier, see TS 23.003 [10].
    - If MSISDN is included in the subscription data, it shall be possible that the same MSISDN value is supported in both 5GS and EPS.

The subscription data for a UE in HSS/UDR may associate the subscriber with groups. A group is identified by an Internal-Group Identifier. A subscription may be associated to one or several External Group Identifier(s) that are stored in the HSS/UDM. When the External Group Identifier is used, the HSS/UDM shall be able to resolve the External Group Identifier to an Internal-Group Identifier.

The NEF or SCEF supports the following independent functionality:

- Exposure of capabilities and events:
- Secure provision of information from external application to 3GPP network:
- Translation of internal-external information:
- It translates between information exchanged with the AF and information exchanged with the internal network function. For example, it translates between an AF-Service-Identifier and internal 5G Core information such as DNN, S-NSSAI.
- In particular, it handles masking of network and user sensitive information to external AF's according to the network policy.
- It receives information from other network functions (based on exposed capabilities of other network functions) and stores the received information as structured data using a standardized interface to a Unified Data Repository (UDR). The stored information can be accessed and "re-exposed" by the NEF to other network functions and Application Functions, and used for other purposes such as analytics.
- A NEF may also support a PFD Function: The PFD Function in the NEF may store and retrieve PFD(s) in the UDR and shall provide PFD(s) to the SMF on the request of SMF (pull mode) or on the request of PFD management from NEF (push mode)
- A NEF may also support a 5GLAN Group Management Function: The 5GLAN Group Management Function in the NEF may store the 5GLAN group information in the UDR via UDM.
- Exposure of analytics: NWDAF analytics may be securely exposed by NEF for external party.
- Retrieval of data from external party by NWDAF: Data provided by the external party may be collected by NWDAF via NEF for analytics generation purpose. NEF handles and forwards requests and notifications between NWDAF and AF.

- Support of Non-IP Data Delivery: NEF provides a means for management of NIDD configuration and delivery of MO/MT unstructured data by exposing the NIDD APIs on the N33/Nnef reference point.

For the support of UAVs in 3GPP networks, 3GPP has defined a new 3GPP UAS Network Function (UAS NF) for support of aerial functionality related to UAV identification and tracking, and to support Remote Identification. The UAS NF makes use of existing NEF/SCEF exposure services to enable UAV authentication/authorization, UAV flight authorization, UAV-UAVC pairing authorization, and related revocation, to enable location reporting, and to enable control of QoS/traffic filtering for C2 communication. Current NEF/SCEF services and APIs are leveraged to the maximum extent.

9.5 Location Services

3GPP system supports the capability of providing location information of a target UE or a group of UEs to the AF or 3GPP LCS (Location Services) client based on the required QoS. The types of Location Request include:

- Network Induced Location Request (NI-LR): With a Network Induced Location Request (NI-LR), a serving AMF for a UE initiates location of the UE for some regulatory service (e.g. an emergency call from the UE).
- Mobile Terminated Location Request (MT-LR): With a Mobile Terminated Location Request (MT-LR), an LCS client or AF external to or internal to a serving PLMN sends a location request to the PLMN (which may be the HPLMN or VPLMN) for the location of a target UE.
- Mobile Originated Location Request (MO-LR): With a Mobile Originated Location Request (MO-LR), a UE sends a request to a serving PLMN for location related information for the UE.
- Immediate Location Request: With an immediate location request, an LCS client or AF sends or instigates a location request for a target UE (or group of target UEs) and expects to receive a response containing location information for the target UE (or group of target UEs) within a short time period which may be specified using QoS. An immediate location request may be used for an NI-LR. MT-LR or MO-LR.
- Deferred Location Request: With a deferred location request, an LCS client or AF sends a location request to a PLMN for a target UE (or group of target UEs) and expects to receive a response containing the indication of event occurrence and location information if requested for the target UE (or group of target UEs) at some future time (or times), which may be associated with specific events associated with the target UE (or group of target UEs). The following types of event are defined for a deferred location request.
    - UE availability: Any event in which the core network has established a contact with the UE. This event is considered to be applicable when the UE is temporarily unavailable due to inaction by the user, or for temporarily loss of radio connectivity or IMSI detach and so on.
    - Area: An event where the UE enters, leaves, or remains within a pre-defined geographical area. The LCS client or AF may define the target area as a geographical area or as a geopolitical name of an area.

- Periodic Location: An event where a defined periodic timer expires in the UE and activates a location report.
- Motion: An event where the UE moves by more than some predefined straight-line distance from a previous location.

LCS Quality of Service is used to characterise the location request. It can either be determined by the operator or determined based on the negotiation with the LCS client or the AF. LCS Quality of Service information is characterised by 3 key attributes:

- LCS QoS Class: The LCS QoS Class defines the degree of adherence by the Location Service to the required Accuracy, if requested. The 3GPP system shall attempt to satisfy the required Accuracy regardless of the use of QoS Class. There are 2 LCS QoS Classes:
  - Best Effort Class: the least stringent requirement on the QoS achieved for a location request. If a location estimate obtained does not fulfil the other QoS requirements, it should still be returned but with an appropriate indication that the requested QoS was not met.
  - Assured Class: This class defines the most stringent requirement on the accuracy achieved for a location request.
- Accuracy: i.e., Horizontal Accuracy and Vertical Accuracy. The accuracy may be mapped to the list of cell ID, gNB/eNB ID and/or TAI, or it may be finer than cell ID. Different LCS procedures may be triggered to achieve either cell ID level or finer than cell ID level accuracy requirements:
  - Cell ID level: The Location Request is sent to AMF to trigger location reporting procedure
  - Finer than cell ID level: The Location Request is sent to GMLC to trigger MT-LR procedure or deferred MT-LR procedure

Response Time (e.g. no delay, low delay or delay tolerant). Location service can be exposed to the authorized control plane NF or the LCS client to obtain the UE location to enable their application and services using the MT-LR procedure. Location reporting is one of the monitoring events as defined in clause 4.4. For the location service exposed to the AF which is not allowed to directly interact with the GMLC or AMF, CAPIF API may be used between NEF/SCEF and the AF. Attributes of location service requests and location service response are defined in TS 23.273 [a].

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, or a control plane NF within a PLMN.

For location request from LCS client (neither in the UE nor in the NG-RAN) or AF external to a PLMN, privacy verification of the target UE shall be enabled to check whether it is allowed to acquire the UE location information based on UE LCS privacy profile and whether the LCS client or the AF is authorised to use the location service. Additionally, UEs may optionally support privacy notification and verification on behalf of a user. Privacy override is also supported for regulatory LCS services according to local regulation. UE LCS privacy allows a UE and/or AF to control which LCS clients and AFs are and are not allowed access to UE location information. UE LCS privacy can be supported via subscription and via UE LCS privacy profile handling.

To provide Location Service in the EPC interworking scenario, an EPC and 5GC common interface shall be used for the location request from LCS client or AF.

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit www.gsma.com

About the GUTMA

The Global UTM Association (GUTMA) is a non-profit consortium of worldwide Unmanned Aircraft Systems Traffic Management (UTM) stakeholders. Its purpose is to foster the safe, secure and efficient integration of drones in national airspace systems. Its mission is to support and accelerate the transparent implementation of globally interoperable UTM systems. GUTMA members collaborate remotely.

For more information, please visit www.gutma.org