UNMANNED AIRCRAFT REMOTE IDENTIFICATION THROUGH CELLULAR NETWORKS

2020

Table of Contents

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 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 the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

GSMA Connectivity for Aviation

The Unmanned Aircraft Systems (UAS) market is one of the fastest growing and innovative sectors of the IoT and presents a huge commercial and strategic opportunity for operators and their technology partners.

The GSMA is actively working with the telecoms and aviation industries to maximise the use of beyond-visual-line-of-sight capabilities of UAS, develop new use cases and help create an open and trusted regulatory environment.

For more information visit: www.gsma.com/aviation

Introduction

Problem Statement

Regulations on identifying cooperative Unmanned Aircraft (UA), frequently referred to as Remote Identification or Remote ID, are beginning to go into effect for different categories of UA. Depending on the country and use case, regulations require a broadcast solution, in others a networked solution, and some may require both. Mobile networks are suitable to fulfil Network Remote ID requirements and this requirements document will provide details about how it can be achieved.

Objective

The mobile industry aims to demonstrate how cellular networks are able to support regulations for Remote ID for different categories of UA, particularly for the European Union's (EU) open and specific categories (United States (US) categories are expected to be quite similar). The objective is to describe how the identification can be achieved with the existing network technologies in the short run, primarily using 4G technologies. The paper will also explain why mobile networks are a very good proposition for Remote ID of UA, and how it has been supported by several Mobile Network Operators (MNOs) globally.

Audience

The paper is intended for all interested ecosystem stakeholders, including: manufacturers, drone operators, pilots, Unmanned Traffic Management (UTM) providers, regulatory bodies, MNOs, etc.

What is Remote Identification?

UA (also known as drone) technology has significantly evolved in the last decade, and UA manufacturers have been providing affordable solutions to consumers. Such evolution has opened the opportunity for many enterprises to consider employing UA to support their operations. For example, Business Insider[1] forecasts that total global shipments will reach 29 million by 2021 for the consumer market and 2.4 million by 2023 for the commercial market – with an impressive 66.8% Compound Annual Growth Rate (CAGR). The growth potential of commercial UA is expected to increase, with the ability to control the UA from a control room instead of a standard Ground Control Station (GCS) connected using short-range communication. The true potential for commercial UA can only be realised by Beyond Visual Line of Sight (BVLOS, sometimes referred to simply as Beyond Line of Sight), but most of these operations cannot be conducted safely with unlicensed spectrum.

Due to the increasing number of UA operations, regulators recognise that most UA should be electronically identifiable for safety and security reasons. The identification of UA is particularly needed to prevent unauthorised operations in restricted airspace, to address suspicious operations near sensitive facilities, and to increase airspace awareness. During the past few years, citizens and law enforcement have been concerned that UA were flying in unauthorised areas or they were infringing upon individual privacy; therefore, regulators needed a mechanism to be able to identify a UA and the pilot. In order to address those concerns, a real time ability to identify UA in the local airspace is needed at any time. In later phases, such identification can support the basic functionalities for coordination of UA flights in UTM; approving flights and collision avoidance; plans ahead of each flight and avoiding conflicting flight plans allowing for modification.

Identification allows governments to have a mechanism to be used as a basis for safety, security, and enforcing rule compliance. The system is analogous to that of vehicle licensing, each vehicle has an identification that is used by governments to identify the vehicle (number plate), and the driver, who is required to have an appropriate driver license, to drive the vehicle. For UA, however the environment itself presents new challenges. Primarily, the inability to check both the identification of the UA and the pilot license physically in person. Although the manned aircraft concept of "N numbers" was considered, UA are generally too small for effective physical identification. Hence the need for what is commonly called a "Remote Identification" (Remote ID) and an automated system that allows authorised personnel to access information on the operation required. Remote ID should be considered the digital number plate for UA, plus the required checks and authorisation to be performed. It should be noted that such Remote ID is considered as a system to support public and air traffic safety in the interest of all involved parties assuming the intention of cooperative behavior. A UA intentionally hiding from identification and detection, so not complying with rules, is not covered by Remote ID but subject to different detection systems. Remote ID provides a capability which allows for UA remote pilots to be accountable for their flying activity by removing complete anonymity, as is often the case today when UA are flying with no ID being broadcast directly from the UA and no ID being sent from the UA via a network connection. However, at the same time as accountability is increased, operational privacy is preserved for remote pilots, businesses, and their customers via procedures described in ASTM F3411-19, "Standard Specification for Remote ID and Tracking"[2].

[1] Drone market outlook: industry growth trends, market stats and forecast - https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts?r=US&IR=T
[2] https://www.astm.org/Standards/F3411.htm

Regulatory Requirements for Remote Identification

UA regulations vary significantly country to country, as regulators try to adapt current laws or develop new regulatory regimes for new UA technologies. Some countries have an outright ban, or an effective ban, on commercial UA. Countries with existing UA legislation are constantly re-assessing the rules and many of those laws have been written or amended fairly recently.

In order to understand the global landscape better, it is important to have an overview of the approaches taken by regulators in different areas of the world and to have a good understanding of the needs of UA manufacturers, operators and pilots. In countries with UA regulations, the rules tend to focus on restricted zones, a pilot's license and insurance, and registration of the drone. There are variations between countries based on UA mass and weight, maximum altitude, population density, and operation type.

Annex A includes an overview of UA regulations in a number of countries around the world, in terms of pre-flight registration and Remote ID requirements.

In terms of pre-flight registration requirements, the overview shows that most countries either have, or are in the process of, introducing requirements on UA identification and registration. Depending on UA weight and flight scenarios, UAs will need to be registered or licensed, typically online, with some countries requiring UA identification to be visible on the UA. In addition to the UA details, pilot details need to be included as well. Some countries require pilots to have a UA certificate, and may include age and residency restrictions.

The subject of Remote ID has either not been addressed yet or is still under discussion in many countries. A Remote ID service typically allows relevant stakeholders to obtain information related to the UA, its pilot and basic flight parameters (location and speed). Where technology for Remote ID has been included in the rules or proposals, most current proposals are technology neutral and include both broadcast and network technologies (EU and US).

Most regulators are only just starting the long process for covering all the aspects needed for a regulation that covers all categories and aspects for obtaining safe operation and eventually a full integration of manned and unmanned air traffic. Remote ID should be considered as one of the first building blocks for defining such a UA regulatory framework.

Unmanned Aircraft Landscape for Remote Identification

It is a common concept in the crewed aviation world for an aircraft to have an identifier that transmits its identity and location of the aircraft to the appropriate control tower; at least in controlled airspace. Identification and position are quite complex and they have been evolving during the years. It is not the purpose of this paper to go in detail about how the system works, but while, radar has been the primary means to enable crewed identification, a more recent solution is Automatic Dependent Surveillance-Broadcast (ADS-B). This started to be deployed around 2008-2009 and is still in progress (e.g. in the US the implementation should be completed by the end of 2020). There are two types of ADS-B: In and Out. With an Automatic Dependent Surveillance-Broadcast (ADS-B) Out system, the information about an aircraft's Global Navigation Satellite System (GNSS) location, altitude, ground speed and other data is broadcasted to ground stations and other aircraft once per second. Air traffic controllers and aircraft equipped with ADS-B In can immediately receive this information sent from an ADS-B Out transponder. This offers more precise tracking of aircraft compared to radar technology, which sweeps for a position information every 5 to 12 seconds. However, ADS-B presents some challenges, which makes it unsuitable for unmanned aircraft. Most importantly, the spectrum used ADS-B has a capacity issue, and it would make it almost impossible to extend its use to the expected high amount of predicted UA due to saturation of the band. In addition, the messages are not encrypted, and therefore the system might raise security and privacy concerns if adopted as is for UA. These are some of the reasons why regulators have preferred industry and jointly developed new systems for the unmanned aircraft. Other technologies are also in place for smaller crewed aircraft, such as the FLARM[3], mainly used in EU. The receiver has a smaller range compared to ADS-B, typically between 20-100 km, but it consumes very little power. Both ADS-B and FLARM require a dedicated ground infrastructure unless the UA is equipped with an onboard ADS-B receiver or FLARM transponder.

Broadcast and Networked Method for Transmitting the Identification

The two methods identified for Remote ID are broadcast and networked. Both methods are required by upcoming regulations and therefore described in this paper. It is important to understand that each method has benefits and limitations and they are considered complementary to cover most of the situations. For example, when the Network Remote ID is used and there is a break in connectivity during the flight, the broadcast method can still be used to provide awareness to the people and other UA in the vicinity. The choice of which method should be used is dependent on several factors, like type of operation, flight zones, use case, etc.

The ASTM Standard Organisation recently released the document ASTM F3411, “Standard Specification for Remote ID and Tracking”[4] which defines message formats, transmission methods, and minimum performance standards for the two methods of transmission of the Remote ID: broadcast and networked. The released document does not provide security for privacy, confidentiality and integrity protection, but ASTM currently has ongoing work on the topic. According to the ASTM specification, there are three methods defined for provide the Remote ID:

[3] https://flarm.com/
[4] https://www.astm.org/Standards/F3411.htm

- Non-equipped: UA operators must report an area of operation prior to the flight via an Application.
- Broadcast Remote ID: for which, at the time of this paper, the standard only described Wi-Fi Aware and Bluetooth as access network[5].
- Network Remote ID: which could be directly from the UA by means of an airborne connectivity module or by relaying the information from the drone by using connectivity from the ground Control System.

This paper will only focus on the latter two, and for the Network Remote ID only on the airborne solution in the UA. This section describes the two methods in more detail and provides simple diagrams to identify the key components of broadcast and Network Remote ID.

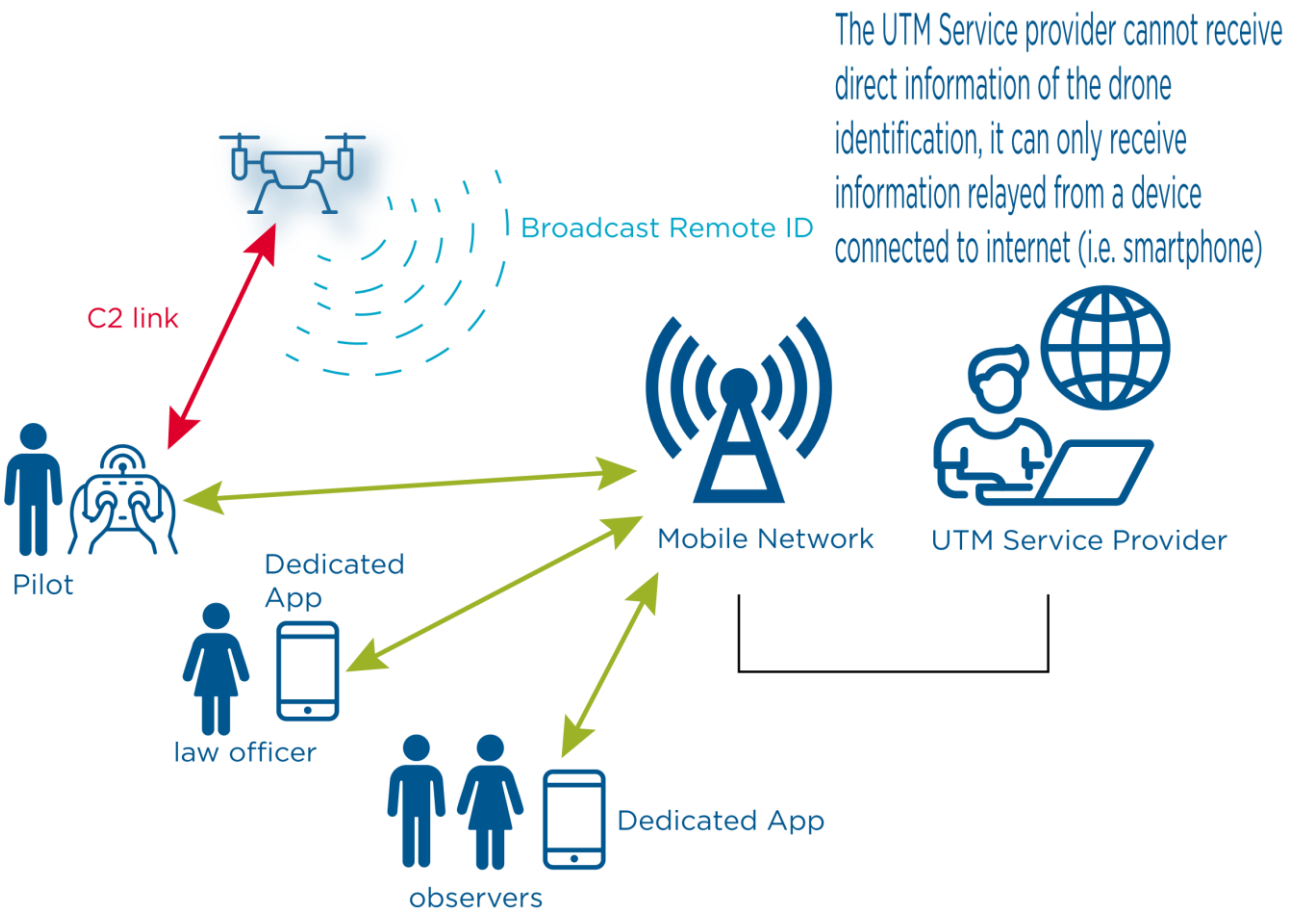


Figure 1: Broadcast Remote ID. Blue dash line for the transmission of the Remote ID; green line for cellular communication; red line for C2 link

Broadcast Remote Identification:

[5] The current published specification includes Bluetooth version 4, version 5 and Wi-Fi Aware. Wi-Fi Aware is also called Neighbor Awareness Networking and at the time of writing of this paper, the technology is not widely available yet. More information about Wi-Fi aware is available here.

As depicted in Figure 1, the UA is regularly sending the identification to the environment, and everybody listening in the vicinity, with the appropriate technology, can receive the signal. It is typical one-to-many communication, which is sometimes also referred to as "local Remote ID". Generally, short-range technologies are used, such as Bluetooth or Wi-Fi. This solution was envisioned in particular to respond to citizens' and law enforcement's concern about UA, used by general hobbyists or nefarious actors, infringing upon privacy or no-fly zone restrictions. Hence the idea to broadcast the information to anyone. Thus, any potential party interested in verifying the identity and location of the UA would require a dedicated application on a device (e.g. smartphone) in order to receive the data directly from the UA, and it would also connect to a UTM Service Provider if more information is needed, e.g. the pilot license. In this scenario, UTM Service Providers and the Air Navigation Service Provider (ANSP) would be unaware of the location of the UA unless relayed through the internet, by monitoring sites or by another connected device, such as the GCS which constitutes as Network Remote ID. Potentially, the information sent from the UA to the GCS could be tampered with if the appropriate security measures are not in place. Also, it should be considered that broadcasting messages is power consuming for both the device transmitting and receiving, particularly for the receiver. More importantly, broadcast technologies are limited in range and the Remote ID would only be visible by anybody in the vicinity of the UA. It should be noted that the identification information can also be delivered by utilising cellular technologies onboard the UA (e.g. Sidelink), the details of which will be explained in further chapters. This method ensures that anyone connected (people with smartphones, other UA, etc) in the surrounding area of the UA are able to get information and it is a complimentary solution to the Network Remote ID.

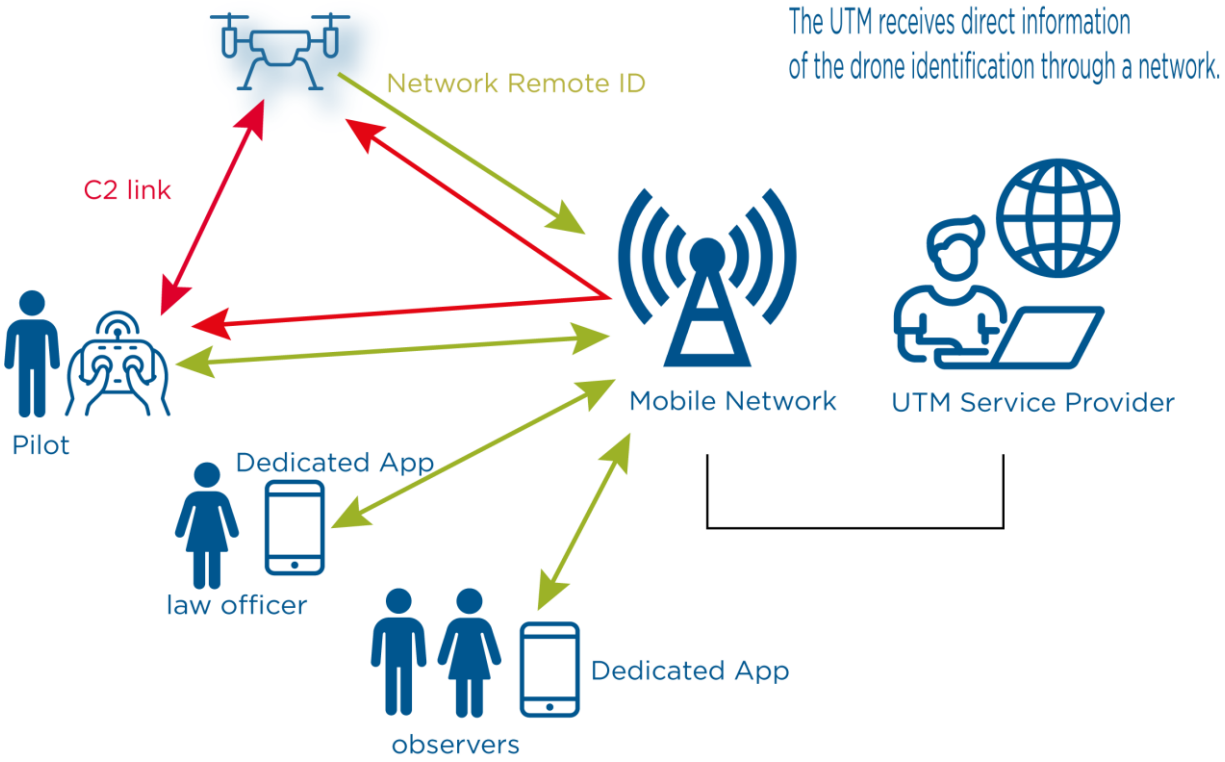


Figure 2: Cellular Network Remote ID. Green line for cellular communication; red line for C2 link (either through cellular or not).

Cellular Network Remote Identification:

In contrast to the broadcast method, Figure 2 describes the cellular networked method for Remote ID. In this example, the UA transmits the information though a communication network directly to the UTM Service Provider, following which the information of all UA in the airspace is available to authorised viewers, and different users could have varying types of data available. A web browser or smartphone with an application could be used to access the data. In this scenario, the communication is a 1-to-1 and not a 1-to-many, as with broadcast Remote ID. The data from the UA will be routed to the UTM service provider and then available on demand. In this case, assuming all UTM service providers are required to share data and be interoperable, interested parties would have a much more complete overview of all UA in the sky. The use of a networked method of transmission is important because it enables BVLOS operation, since the UTM service provider receives near real-time information about the specific UA, then such information is available to any other authorized stakeholders. Thus, supporting an internet-based Network Remote ID is the foundation for supporting safe BVLOS operation.

Any means of connecting to the internet, such as satellite and aviation bands, can be used as an alternative types of communication, but, for the purpose of this paper, cellular connectivity is the focus. Thus, it is called Cellular Network Remote ID.

Remote Identification Security and Privacy Considerations

When considering identification and positioning information there are a common set of questions about security and privacy. If we look at manned aviation, the identification and the position of the aircraft are available for everybody. ADS-B does not support encryption, while FLARM does offer a proprietary encryption. Drone operators and pilots are concerned that their personal information or their drone's location could be exposed, and that they might be vulnerable to attacks. And that the drone location might reveal sensitive information about the commercial usage (e.g. location of their customer in case of delivery). Given that the ecosystem of stakeholders is complex, it is important to understand what information is proposed to be visible, to whom, and what can be exchanged with other parties. In addition, to provide adequate cyber security protection options. However, this challenge is at odds with the communication methods for the Remote ID. Ultimately, it is up to the regulatory authority in each country to identify specific regulatory details.

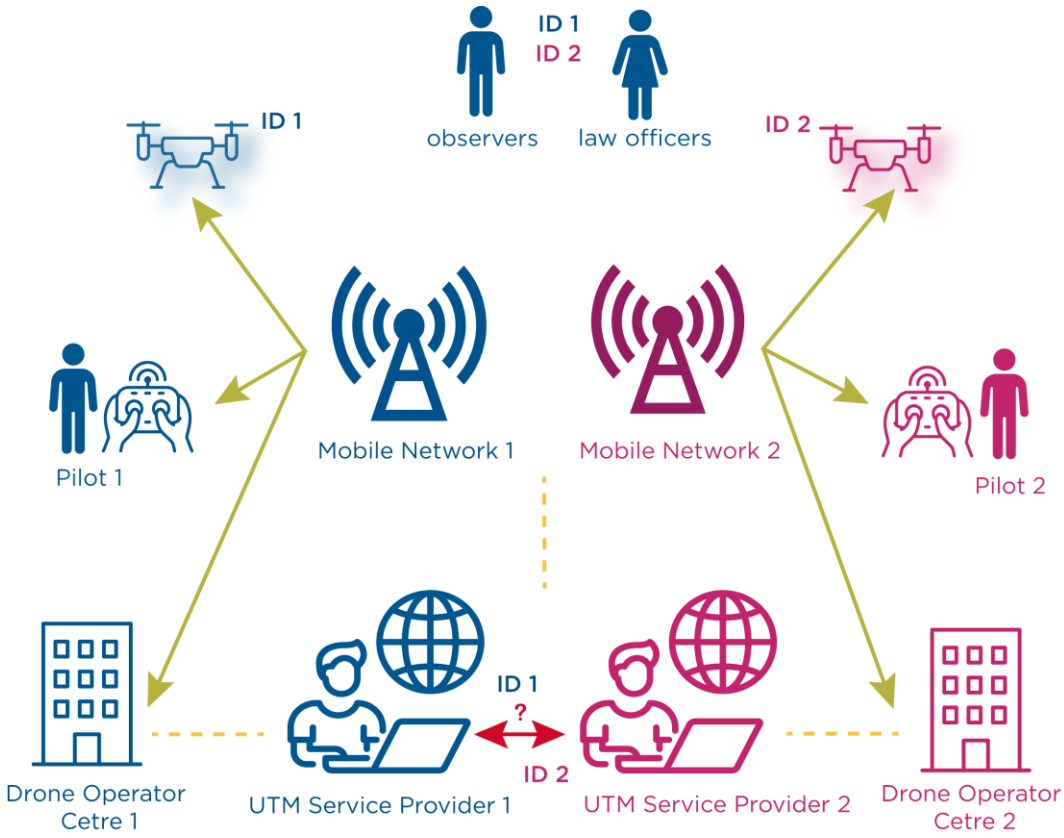


Figure 3: Interoperability between different UTM Service Providers

Figure 3 provides a very simple overview of the different stakeholders in order to understand what information should be provided to each of them. The scenario depicted assumes that there are multiple UTM service providers in a given country or territory, and a drone operator/pilot has the choice to choose any of the available UTM service providers. Drone operator 1 has a subscription with the UTM provider 1, and drone operator 2 with UTM service provider 2. In this example, each operator also uses a different mobile network. Each drone operator is allowed to see all information carried in the Remote ID from their UA. However, it is still unclear what amount of information can be provided to other parties connected to the serving UTM provider, as well as how it should be exchanged (API). For example, is an observer, such as a law enforcement officer or another UTM service provider, allowed to view all information from the Remote ID, or only a limited set? Since the Remote ID might also include the location of the pilot, it could be envisaged that this information is only provided to authorised people or a specific entity, but not to anybody else.

At this stage it is assumed that it is the responsibility of the drone operator/pilot to make sure that the information is received appropriately by the UTM service provider. A regulatory framework should clarify these questions and some countries are looking at manufacturing requirements to ensure Remote ID capability, but the general framework is important for understanding the responsibility of each party and to build an appropriate security and privacy framework.

Remote Identification through Cellular Networks

The existing capabilities of mobile networks can enable the safe operation of UAs, which are becoming increasingly popular with consumers and businesses. The GSMA Mobile Economy[6] paper reported that in 2019 there were about eight billion cellular connections for traditional devices and 12 billion cellular connections for Internet of Things (IoT) devices globally. The forecast for 2025 expects the number to reach about 8.8 billion consumer devices and so double the IoT connections. Thus, even if consumer devices are still the primary devices connecting mobile networks, is it clear that these networks are constantly evolving and improving in order to better support the growing number and variety of devices, and UA are expected to remain a fraction of the connections for some time. Mobile networks are constantly evolving to support the emerging services and needs of multiple industries. Many MNOs have already deployed 4G Long Term Evolution (LTE) networks, which can deliver high-bandwidth, low latency connectivity with an exceptional quality of service which is designed to scale. 4G networks offer a wide range of capabilities that can be used by the UA industry and also for the Remote Identification. The next evolution of mobile technology, 5G, is designed to connect many more devices, while delivering even faster transmission, lower latency, and higher predictability and stability in the communication.

For the cellular connectivity for Remote ID of UA should offer:

- Scalable solution, suitable for mass market: Given the high number of connected objects, any solution must be able to support the rapid growth in UA and to deliver a high capacity in the future.
- High reliability and availability: A high safety level is crucial for any implementation, which should also be widely available.
- Light and easy to integrate solution: Commercial off the shelf solutions are needed and they must be efficient and dependable: low cost solutions with a low level of complexity and proven track record will be in demand.
- Ready for implementation as soon as possible: UA are already flying in the airspace, so Remote ID needs UA to be safely and fairly integrated into air traffic management as soon as possible and available to both new and existing UA.

Mobile Networks have a variety of assets and capabilities to fulfil these requirements:

- Standardised and scalable solution for worldwide connectivity: Mobile networks are used by billions of devices worldwide, and generally operate on harmonised and standardised technologies defined by the 3rd Generation Partnership Project (3GPP)[7].
- Globally available, mobile networks provide a solution on existing infrastructure: It is not necessary to roll out a new infrastructure. In addition, mobile networks continue to evolve to match the changing needs of UA communication platforms. Minimal investment is needed to implement the Remote Identification technology.

[6] https://www.gsma.com/mobileeconomy/

[7] http://www.3gpp.org/

- Licensed spectrum: Working with dedicated spectrum in licensed bands enables mobile networks to provide the reliable connectivity required for mission-critical applications, especially in BVLOS cases and in high-risk environments.
- Secure communication channel: Mobile networks provide specific encryption mechanisms to protect communications against misuse, achieving high standards of data protection and privacy.
- Law enforcement: Cellular networks have a history of responding to and supporting lawful governmental investigations and carriers generally do not condone use of their networks for illegal purposes.
- Augmenting the identification through the Subscriber Identity Model (SIM) credentials and International Mobile Equipment Identity (IMEI): Cellular networks have a very stable and proven framework for trusted identification and security, which can be utilised to strengthen Remote ID security.

Utilising the existing mobile networks will eliminate the need to deploy a new infrastructure and, therefore, help to ensure connected UA are economically feasible.

The following section will first look at all capabilities at disposal of the MNOs today and then move to look at future and envision what 5G will bring.

Communication Options for the Cellular Remote Identification

This paper has introduced two methods of transmissions for the Remote ID: Broadcast and Network. This section will illustrate how both methods can be fulfilled by cellular technologies.

Broadcast Remote Identification

Utilising the current capabilities of mobile networks, an LTE-enabled UA has at two different technologies for transmitting the Remote ID in a broadcast fashion:

- LTE Device 2 Device (D2D): this is a technology that has been introduce by 3GPP to allow devices to communicate without a network; the feature has been used for public safety applications (emergency services).
- Sidelink Communication: it is an enhancement from the D2D connectivity between mobile devices, which was introduced for the first time in 3GPP Release 12 for supporting requirements for vehicles communication from other industries, such as automotive and UA. The advantage of Sidelink communication is the ability to be used even when devices are not in coverage of the cellular network. A specific Sidelink solution has already been adopted in automotive for C-V2X.

As with any broadcast technology including Wi-Fi (cellular-related broadcast, Bluetooth, etc.); range; the amount of data transmitted; privacy; the complexity of the UE; and power consumption (particularly for the receiver side) are all critical considerations. The device will transmit the content using a specific frequency and channel, and all the other devices that are listening should scan constantly the spectrum to see if there is anything coming. In the case of using a predefined frequency band (e.g. 2.4 Ghz Wi-Fi), if a lot of devices transmit at the same time on the same channel by chance, there is a risk of collision and the message will get lost. Statistically the chance of collision increases when the number of devices using the same channel increases, and therefore it is recommended to be aware of the collision detection or collision avoidance mechanism and performances of the technology used, either Bluetooth, Wi-Fi or cellular connectivity.

Network Remote ID

In this scenario, the communication from the UA is one-to-one rather than one-to-many; which is the traditional communication options that we are all using in our smartphone, and it is the most used communication mode in the current mobile networks. Figure 4 illustrates the typical secure communication by utilising Access Point Name (APN).

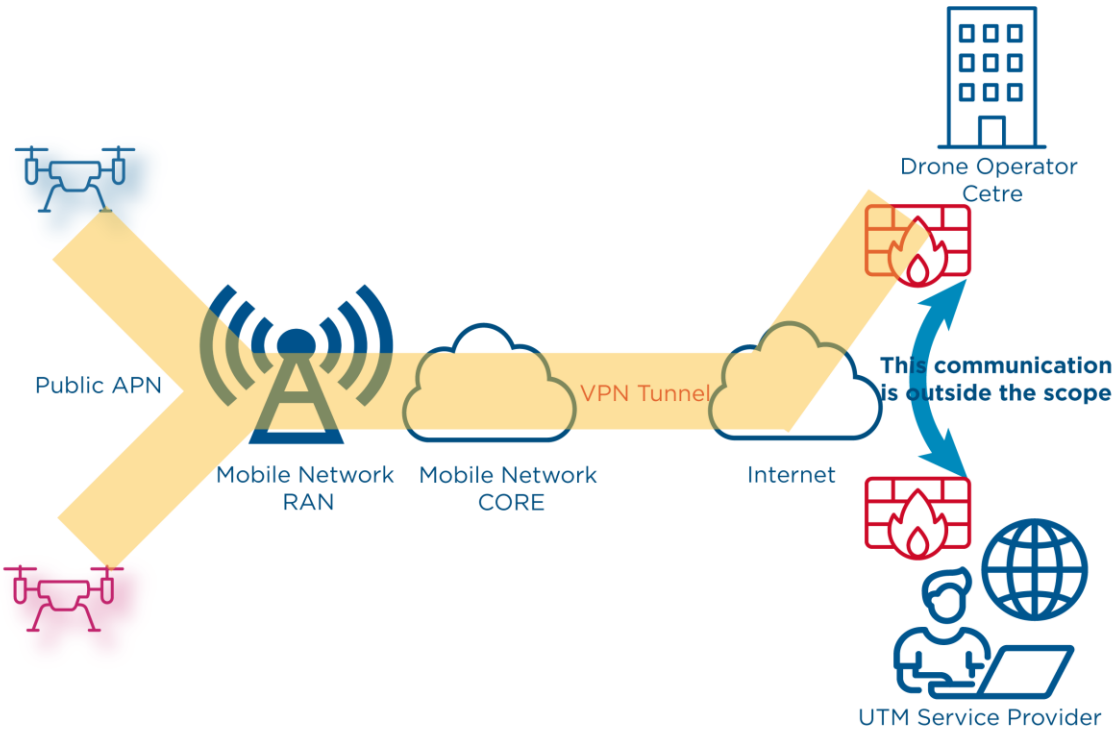


Figure 4: Secure communication with APN

The APN identifies the Packet Data Network (PDN) that a device (UA) wants to communicate with. It is effectively the name of the (virtual) gateway between a mobile network and another network, as shown in Figure 4. In general, it is possible to have public and private APNs.

A public APN is shared by many customers. A good example of such an APN is the one provisioned in smartphones for accessing the internet. In this case, all UA would share the same APN to access the internet and the routing would be done with the specific Internet Protocol (IP) address provided in setting up the communication. This scenario is the one depicted above where in combination to the APN, the IP address of the drone operation centre is provided to route the information appropriately.

A private APN is private to one customer as depicted in Figure 5. Only the SIM cards of that customer can access such an APN. There might be several reasons why a private APN would be the preferred solution, but usually there are technical reasons for owning one and primarily for security purposes. For example, by using a private APN a customer has the following benefits: ability to configure the various

settings, security, setting company specific policies. However, the drawbacks of using a private APN include increased cost, but in most cases, no VPN tunnel is needed since the routing is secured and the data is encrypted end-to-end, thus reduced configuration.

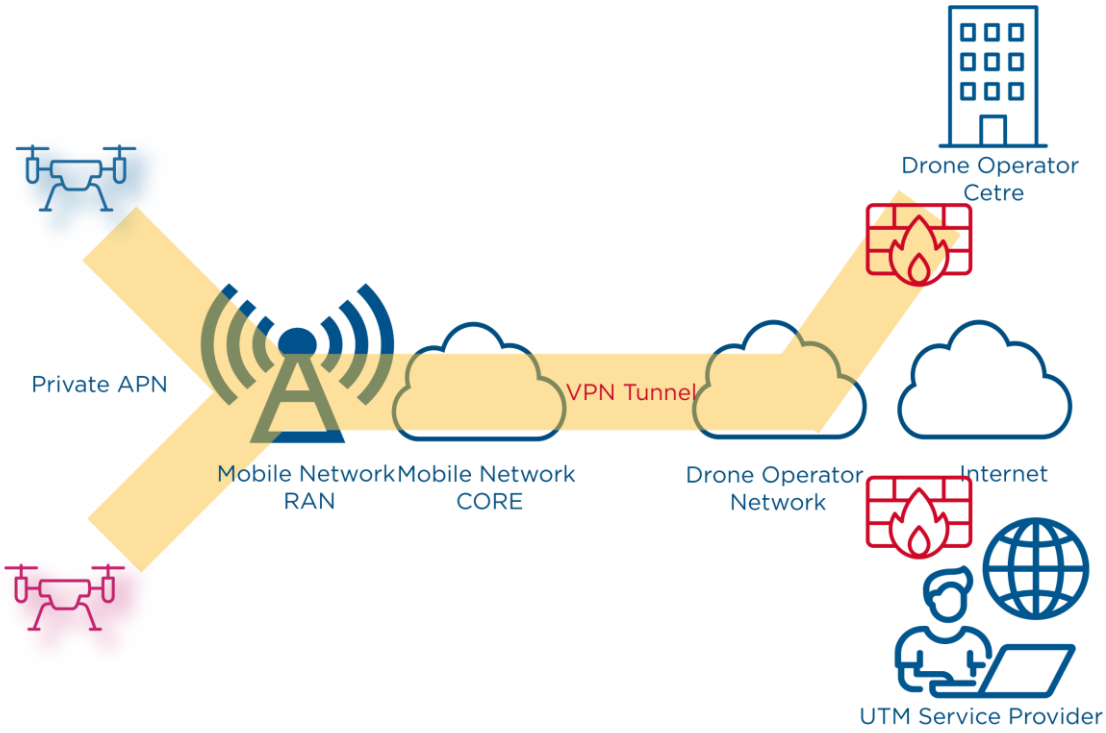


Figure 5: Private APN

In both scenarios, public and private APN, the communication can be either through a VPN tunnel or not. The main benefits of using VPNs are security related features:

- Confidentiality and privacy: preventing 'man in the middle' attacks.
- Authentication: verifying that the sender is a legitimate device and not a device used by an attacker.
- Data Integrity: verifying that the packet was not changed as the packet crossed the internet.
- Anti-replay: preventing a 'man in the middle', from copying and later replaying the packets previously sent by an authorised device, to make an unauthorised device appear legitimate.

The other aspect to consider in setting up the communication is looking at which technology and transport protocol is suitable for transporting the information needed for the Remote ID. The following are all technologies that are capable of delivering the information:

- LTE and Long Term Evolution Advanced (LTE-A)
- Long Term Evolution for Machine type communication (LTE-M)
- Narrowband IoT (NB-IoT)

- Universal Mobile Telecommunications System (UMTS)
- High Speed Packet Access (HSPA) and HSPA+
- General Packet Radio Service (GPRS)

Generally, it is the choice of each individual MNO, which is the technology choice. Ideally, it is recommended to adopt the technology that would offer the best coverage in the specific geographical area. In 2020 4G is already serving more than half of all global connections[8], however there are regions where this is not the case. However, it is also good practice to have other connection options in areas where there is limited LTE. It should be noted that a high number of the available modules do support a variety of options.

Augmenting the Location Information through Cellular Connectivity

As part of the Remote ID, the upcoming regulations also require the location information of the UA. Such information is normally delivered by using a GNSS built-in to the UA, either separate or integrated, with a connectivity module. The US is considering using barometric pressure for altitude. GNSS signals are relatively weak and are vulnerable to jamming, spoofing and the effects would be the absence or false location information reported to UA operators and UTM providers.

Mobile networks offer positioning solutions that will allow independent verification of the location reported by the UA, so that UA operators and UTM providers have a higher level of trust about the information. LTE supports a variety of network-based location solutions such as:

- Cell ID: a mechanism available since 3GPP Release 9; it is the basic location information method and it is available in all networks. The network is aware which Cell ID the UE is attached to (or was last connected to), hence it provides the location of the UE. This method is also the one with the lowest accuracy because the location information would be indicated within a certain radius of the tower. The radius of the geographical areas will also vary depending on frequency and actual location of the tower. For example, cells are smaller in urban environment compare to rural environment.
- Enhanced Cell ID (E-CID): also available since 3GPP Release 9, whereby the User Equipment (UE) can report the strength radio reception, more specifically the reference signal received power and quality (Reference Signal Received Power (RSRP)/ Reference Signal Received Quality (RSRQ)), and the reception and transmission time difference along with the serving cell ID (as per previous method). The added information improves the accuracy.
- Observed Time Difference Of Arrival (OTDOA): also a method available since the 3GPP Release 9. In this case, the modem measures and reports the difference in arrival times of special signals transmitted by all cell sites. More precisely, the estimation of the UE's position is based on a multilateration method in which the UE calculates the difference between the measurements form the Reference Signal Time Difference (RSTD) received by several Evolved Node Bs (eNodeB). Then the UE sends the information to a function in the network called Serving Mobile Location Centre (SMLC) that with the knowledge of the location of the eNodeBs and the time differences sent by the UE is able to calculate the position of the UE.

The accuracy of the location information provided by the methods above are lower than what is achieved with GNSS. Generally, it is not possible to reach the level of a metre or sub-metre accuracy for an LTE network. The location information can be requested on-demand, with a period subscription, or a combination of both. In general, location services are well developed and supported in the scenario where the UE is served by the MNO which is subscribed to; while roaming to another MNO the quality of

[8] The 2020 GSMA Mobile Economy: https://www.gsma.com/mobileeconomy/

service provided may vary (e.g. dynamic environmental conditions, service quality, roaming partner's network not supporting the same location method or the service may not be available in a roaming partner's network).

These capabilities, standardised by 3GPP, are part of a common framework known as the Location Services (LCS) [9] [10]. The above mentioned methods are the most commonly deployed, but there are other methods described in the specifications. These specifications describe the mechanisms by which measurement reports are provided to the network, but not the algorithm by which location is estimated. Hence, there remains scope for innovation and, through the GSMA, MNOs are interested to develop these services and work together with UA stakeholders to ensure compliance with UTM requirements.

Improved Security by Using Mobile Networks

Several aspects need to be considered for securing UA communication and protecting data. Mobile networks can help to achieve a secure system for delivering the Remote ID. Some examples are listed below:

- Secure registration of pilots and their UA: The registration of pilots and their UA to public authority servers needs to be secure and reliable. This is the first step for ensuring trusted flights. Public authorities need to verify the pilot's ID and check that they hold a valid license, if applicable. They also need to link each UA with a pilot, just like a vehicle's license plate links it to the owner of the vehicle, so if the UA goes off course, for example, the authorities can contact the UA immediately. In some cases, mobile networks can support the pilot registration by using the existing SIM registration mechanism (however it should be the pilot who undergoes the registration and not the owner of the UA/SIM). It should be noted that not all countries require SIM registration, but where available it would offer a simple and established mechanism to be easily extend to the UA ecosystem.
- Protection of data: Remote ID could be regarded as sensitive data since it contains information about the location of the UA and the location of the pilot. Mobile networks provide secure communication from the UA and the network, while allowing the service provider to encrypt end-to-end the data up to the edge of the mobile network. The GSMA IoT Security Guidelines[11] make several recommendations based on a risk assessment.
- Seamless and secure connectivity: For easy deployment worldwide, manufacturers need to be able to connect their UA seamlessly and securely to networks in any country. Mobile networks provide secure connectivity around the world.
- Reliable UA location: UA operators, UTM service providers and public authorities need to be able to identify UA and reliably locate them, anywhere in real-time. The UA location data comprises digital IDs, such as serial numbers, and any related data (such as location, time, pilot, etc.), and this data must not be modified during the flight. The location of the UA will be provided by GNSS systems, but it could be tampered with, or inaccurate or not present. Mobile networks can securely provide the correlation of location information and other state information to ensure greater assurance and resilience in critical UA operations.

[9] 3GPP TS 23.271 - Functional stage 2 description of Location Services (LCS)

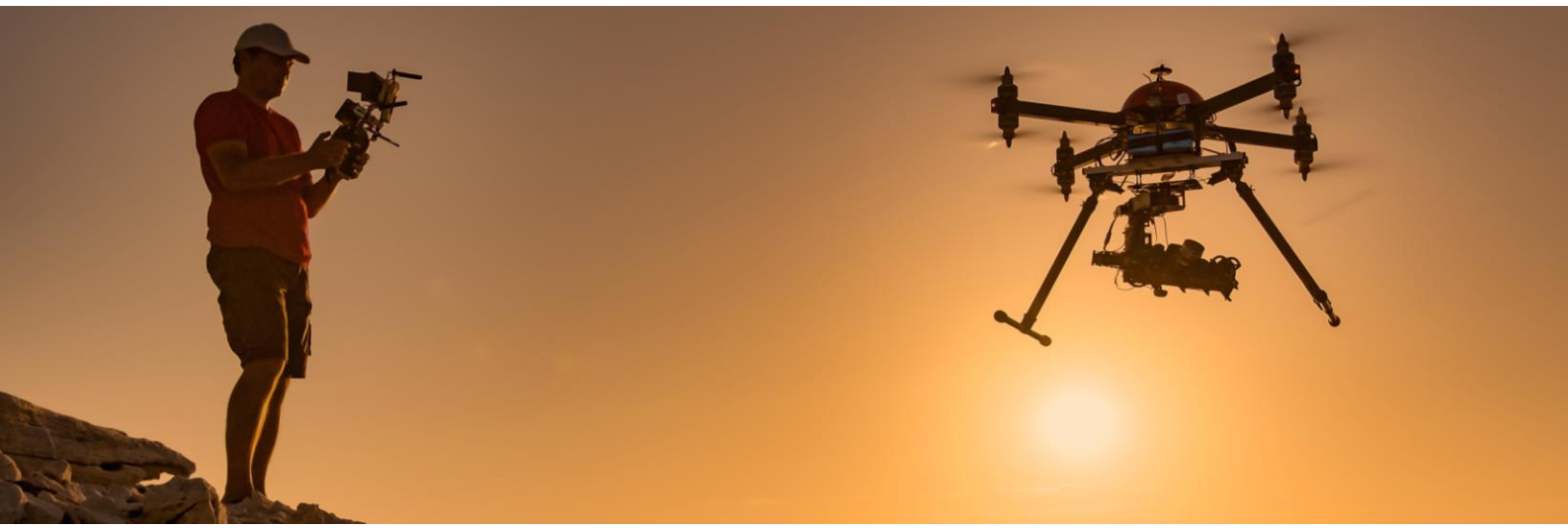
[10] 3GPP TS 36.305 - Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRAN

[11] GSMA IoT Security Guidelines and Assessment; https://www.gsma.com/iot/iot-security/iot-security-guidelines/

Summary

The growth of consumer and commercial UA is taking place, but right now there are limitations on commercial UA flights; notably the need for regulatory guidance to the ecosystem stakeholders on how to plan for the future operations where pilots will be able to operate UA BVLOS. UA could be used for many new applications, such as inspection and surveys, transport and logistics, surveillance and monitoring, and communications and media. Safe BVLOS operations would also enable UA to play a much greater role in disaster response and law enforcement, as also demonstrated during the Covid-19 pandemic that the world experienced during 2020. The vision is to be able to move to enable full automation, which could reduce the operating cost per mission and increase safety. The first step to automation is the ability to identify and know the location of the vehicles in the sky, hence the importance of the Remote ID. Regulations in different countries of the world are progressing at different speeds, but it is clear that most of them are tackling the Remote ID and the need to have standard solutions. Cellular networks are a widely deployed infrastructure that can make the deployment of UA easy and trusted, allowing Remote Pilot In Command (RPIC) to safely manage all the vehicles in the sky and spur innovation.

Systems will be needed to manage the multitude of flying objects, some acting autonomously, some periodically controlled, or at least, supervised by a remote operator and all monitored to ensure full control and integration with the general air traffic. Both national and international authorities are investigating the development of a new UTM for unmanned operations that is separate, but complementary, to the existing ATM systems used for commercial aircraft. Wireless connectivity will be able to deliver many facets of UTM, starting from identification and further in the future to provide information to support flight planning and approval, the transmission of meteorological information, geo-fencing, geo-caging and more. Cellular technologies, such as LTE and 5G, are reliable, secure and cost-effective and not only are they suited to support the needs of a Remote ID, but they could help enable BVLOS operation of UA and ultimately full automation with a variety of capabilities and services that can be utilised pre-flight preparation and during flight. The GSMA paper "Using Mobile Networks to Coordinate Unmanned Aircraft Traffic"[12] explores in detail the services that MNOs can offer to support a safer and more effective flight management for UA at low altitude. For a comprehensive overview on how mobile networks can support UA operations refer to the GSMA "Mobile-Enabled Unmanned Aircraft".[13]



[12] https://www.gsma.com/iot/wp-content/uploads/2018/11/Mobile-Networks-enabling-UTM-v5NG.pdf
[13] https://www.gsma.com/iot/wp-content/uploads/2018/02/Mobile-Enabled-Unmanned-Aircraft-web.pdf

Remote ID Demonstrations

Report on Remote ID Demonstrator from the Swiss U-Space Implementation

In December 2018 Switzerland formed the Swiss U-Space Implementation (SUSI)[14], a public-private partnership with the purpose to identify, quantify, develop and implement the U-Space capabilities and technologies in Switzerland. One of the first demonstrations (September 2019) was focused on assessing the ASTM standard for Remote ID. At the time of the demonstration the ASTM standard was not yet finalised, however it provided very insightful feedback[15]. The demonstration was conducted by six industry participants, members of the SUSI program: ANRA Technologies, Airmap, Involi, Orbitalize, skyguide, and Wing. Both solutions broadcast and networked ID worked as expected. For broadcast four technologies were utilised: Bluetooth 4, Bluetooth 5, Wi-Fi Aware and also Wi-Fi Service Set Identifier (SSID). The technologies proved to work properly, but the demonstration faced challenges on the availability of these technologies either on smartphones or UA that are currently in the market. The networked ID solution worked as expected without any further complications.

Swisscom Proof of Concept on Cellular Network Remote ID

Swisscom, also in Switzerland, performed in December 2019 a Proof of Concept to demonstrate the cellular Network Remote ID with the integration of FLARM to also capture lower altitude manned aviation traffic. The Remote ID is also inspired by the ASTM standard and the target architecture of the Proof of Concept is shown in Figure 6.

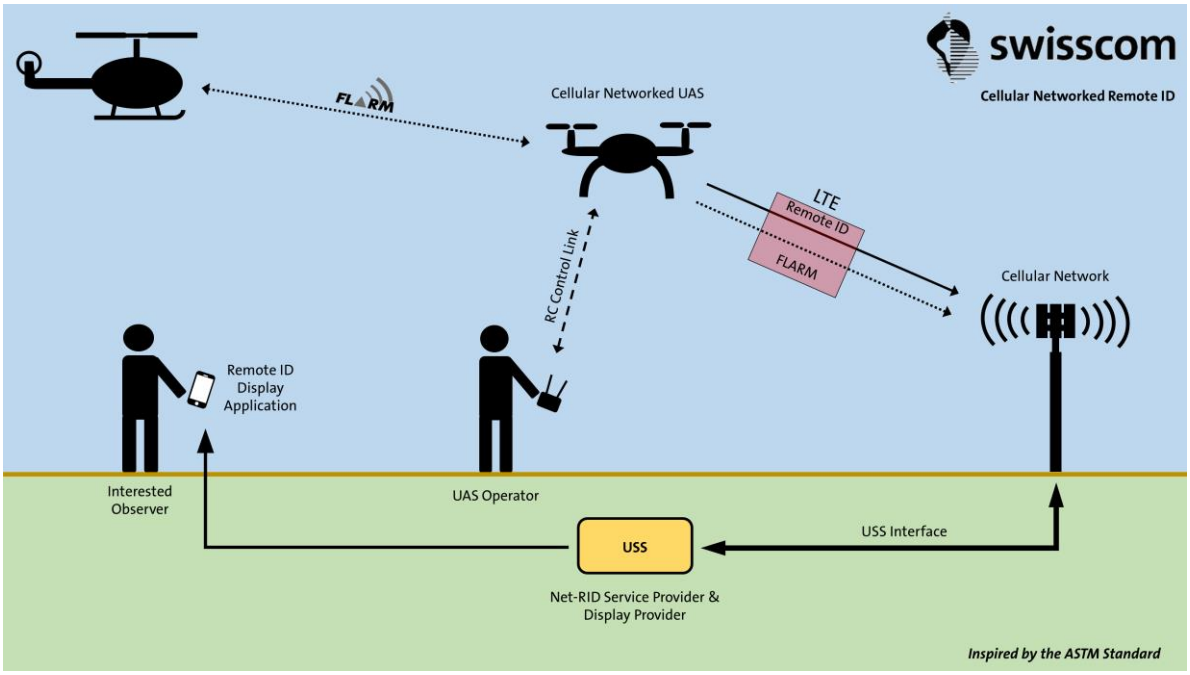


Figure 6: Swisscom Proof of Concept Architecture for Cellular Remote ID

[14] https://susi.swiss/#:~:text=SUSI%20is%20a%20Public%2DPrivate,and%20UTM%2FU%2DSpace.
[15] Full report of the demonstration available here: https://susi.swiss/2019/09/16/remote-id-demonstration-report/

The UA is equipped with a prototype of the self-contained Swisscom Cellular Network Remote ID Device, see Figure 7.

The device is designed to send the ID, position, altitude, and other information periodically to U-Space (USS in Figure 6) and allows for constant tracking & tracing. There are plans for a market-ready product to fully integrate with ASTM remote ID standard such that the information sent to the Remote ID service provider can be visualised by any display provider application regardless of the user's location and regardless of a direct communication link between the application and the UA. The communication is using licensed spectrum on established LTE infrastructure of Swisscom. In addition, the Swisscom cellular Network Remote ID device acts like a regular FLARM transponder by transmitting its FLARM beacon which can be received by any nearby FLARM equipped aircraft such as a rescue helicopter.

Figure 7: Swisscom Cellular Network Remote ID Device

The device also receives FLARM beacons from nearby aircraft and relays the associated traffic information via LTE to the U-Space. Swisscom believes that adding FLARM to the Swisscom cellular Network Remote ID device greatly improves airspace safety and situational awareness by collecting information about traffic in the lower airspace for both U-Space and manned aviation.

Swisscom highlights the following characteristics of cellular networked ID:

- Unlimited range, independent of distance to UA
- Allows integration with safety-relevant systems (FLARM, ADS-B etc.)
- Country-wide cellular coverage, available today
- Licensed spectrum, international standard/roaming, proven for years
- Bidirectional and secure communication
- No further requirements on display app except access to the internet

A video of the Proof of Concept is available at the following link: https://bcove.video/2PcCLDN

US Demonstrator on Networked Based Remote ID

The demonstration took place in September 2019 in a controlled airspace near San Francisco International Airport, and featured participants from Verizon, Skyward, Wing, Uber, AirMap, AiRXOS, ANRA, CNN, Kittyhawk, UASidekick, and Flite Test[16]. Permission to fly in controlled airspace was obtained from the Federal Aviation Administration (FAA) via Low Altitude Authorization and Notification Capability (LAANC). The Network Remote ID was also based on the ASTM standard and the demonstration focused on network-based Remote ID of UA with the InterUSS Platform. The InterUSS Platform[17] is a distributed system that allows connection between multiple UAS Service Suppliers (USSs) operating in the same area to share information while protecting operator and consumer privacy. The demonstration had seven drones flying, supporting different type of use cases including infrastructure inspection, delivery, and recreational flights.

In the demonstration, Verizon and Skyward, a Verizon company, simulated a BVLOS infrastructure inspection flight. The drone utilised Verizon 4G LTE connection for the duration of the flight. The demonstration successfully proved the Network Remote ID based on the ASTM standard and the inter-USS communication. A summary video of the event is available at the following link: https://youtu.be/PeJpC3o8JBM. The demonstration was performed before the FAA released the Note of Proposed Rule Making (NPRM) and it was mainly focusing on the implementation of the ASTM standard.

Figure 8: From demonstration of network based drone Remote ID

[16] https://skyward.io/verizon-skyward-wing-and-others-demonstrate-network-based-drone-remote-identification/
[17] InterUSS Platform is an Open Source Project from Google that implement the Discovery and Synchronization Service (DSS) as described in the ASTM remote ID standard. Project available here: https://github.com/interuss/dss

Annexes

Annex A. Unmanned Aircraft Regulation across the Globe

The following table provides an overview of the UA regulations in selected countries. The information covers two aspects of the regulations: the pre-flight information for registration and the in-flight information for the Remote ID.

Country	Legal source	Provisions on pre-flight UA registration and ID	Provisions on remote UA ID
Australia	Civil Aviation Safety Authority (CASA)	CASA introducing a drone registration and accreditation scheme. UA and model aircraft > 250 g will need to be registered. Accreditation needed if flying a drone or model aircraft > 250 g. The registration requirement took effect on 30 September 2020.	No requirements yet
Canada	Transport Canada	Must follow the rules in Part IX – Remotely Piloted Aircraft Systems Highlights are: • Pilot certificate required for UA weighing 250 g up to 25 kg • Drone must remain within LOS of pilot • UA above 250 g must be registered and marked • Drone must fly no higher than 122 meters above ground level Restricted flying areas applies.	No requirements yet.
China	Civil Aviation Association of China (CAAC)	Regulations on real name registrations of civil unmanned aircraft systems (May 2017) Requirement on manufacturers to provide information about UA and buyers and provide stickers with markings. Requirement on owners to register and place stickers on UA.	No requirements yet. Discussed in a China-EU workshop in May 2019 focusing on U-space development. It mentions the three main UA management systems around the world: • UTM led by the US; • U-space management led by Europe;

			• UAS Operation Management system (UOM) by China. In December 2017, the Ministry of Industry and Information Technology (MIIT) issued guidance proposing research and the introduction of drone digital ID rules and technical solutions (each drone shall have a dedicated ID). Enterprises encouraged to add communication modules for civilian UA to implement ID, monitoring, and management.
European Union	Commission Delegated Regulation (EU) 2019/945 Commission Implementing Regulation (EU) 2019/947 (Art. 12-14) More relevant EU regulation is upcoming on U-Space and Standard Scenarios in the specific category	By January 2021 Member States must implement a national registration scheme. The schemes must be interoperable within the EU. A unique digital registration number must be displayed on each drone. Three categories are distinguished: 1. Open; 2. Specific; 3. Certified. All UA operators in specific category and some (>250g, or potential to have impact of > 80 Joules) in open category need to register as well. Certified category has different requirements and is regulated in existing manned aviation regulation. For a specific category, standard scenarios only require declaration (no authorisation). Two scenarios: 1. Urban VLOS; 2. Rural BVLOS above control ground area operations (up to 120m, weight up to 25kg).	Source: EASA Opinion on Standard Scenarios in the Specific Category (p.23) Remote drone ID is required for all UA intended to be operated below 120 m, to address primarily the security and privacy risks. The requirements for a 'network' Remote ID system are being developed as part of U-space. Network Remote ID mainly developed to address the safety risk (but can also help to address security and privacy risks). It was decided to keep the requirement flexible and mandate for all UAS to be operated in Very Low Level (VLL) airspace, so a Remote ID system will be required to transmit data either 'direct' or 'network'. Reiterated in EASA Opinion 01/2020 High-level regulatory framework for the U-space (p.16):

			It is specified that U-space service providers shall be able to receive and exchange broadcast and network information. This is consistent with the upcoming amendment to Regulation (EU) 2019/945 and supports redundancy under certain use cases, although limited to certain cases of U-space airspace implementation.
Finland	Finnish Transport and Communications Agency (TRAFICOM)	TRAFICOM regulates the use of the aircraft radio transmitters, including unmanned aircraft, and grants the respective licenses. The exceptions include devices of the terrestrial mobile communication systems or electronic communication services on unmanned or other aircraft if they are needed for specifically defined cases of the public administration, health care, public safety, law enforcement, and essential maintenance tasks. Also, GSM or LTE devices on 1710-1785 MHz, and UMTS devices on 1920-1980 MHz can be utilized in the altitude of at least 3 km on an aircraft that operates a base station as defined in the EC resolution 2008/294/EY and 2013/654/EU, and EU regulation 2016/2317. All the other cases require an approval of the TRAFICOM.	As defined by the EU.
France	Draft law on technical requirements for drone identification	Mandatory drone registration and mandatory training for remotely piloted aircraft of mass ≥ 800g (Law n° 2016-1428, updated December 2018). UA weighing more than 25kg must be properly licensed.	The law (Arrêté du 27 décembre 2019 définissant les caractéristiques techniques des dispositifs de signalement électronique et lumineux des aéronefs circulant sans personne à bord) mandates use of Wi-Fi for drone identification (December 2019, paragraph 9).
India	National Drone policy effective from December 2018 (flying UA	Operators need to request a unique Identification Number (UIN)/ Unmanned Aircraft Operator Permit (UAOP), as applicable, from the Director General of	No requirements yet.

	previously prohibited).	Civil Aviation. Exemptions are available for certain categories.	
Italy	A collaboration between ENAV (ENAV UA services) and ENAC (Civil Aviation Drone regulation) created a platform for providing traffic management services to their users called D-Flight.	Since July 2016 both registration and identification of UA and owners has been required. Devices with operating take-off mass greater than or equal to 25 kg shall be registered, by assigning dedicated registration marks and identical registration marks are to be shown on remote ground pilot stations. The identification plates shall be installed on RPA and on remote ground pilot stations. The English translation of the regulation 'Remotely Piloted Aerial Vehicles' (updated in 2018): https://www.enac.gov.it/sites/default/files/allegati/2018-Lug/Regulation_RPAS_Issue_2_Rev_4_eng.pdf	Article 8.2 of Remotely Piloted Aerial Vehicles: Since July 2016, in addition to plates required by Art 8.1, any UAS shall be equipped with an electronic identification device, that allows the transmission of UAS real time data, its owner/operator and basic flight parameters, as well as the recording of these data. Electronic identification device performances and characteristics are defined by ENAC.
Japan	Government announcement only	The government will start policy work on drone registration in 2020 including revising the Civil Aeronautics Law. Drone owners and operators will be required to register name, address, drone manufacturer's name, model, manufacturing number, weight and other data on a government website. The registration requirement covers aircraft already in use or brought to Japan from abroad. The government will issue registration numbers, and the owners will be required to display the numbers on the surface of their UA. Unregistered UA will be prohibited from flying, although aircraft weighing less than 200 grams will not be subjected to the mandatory registration.	No requirements yet
Rwanda	Rwanda Civil Aviation	All UA that are brought to Rwanda must be registered using form RCAA-	No requirements yet

	Regulations Part 27 (Feb 2019)	Form-UAS001. Only citizens and permanent residents of Rwanda who are 21 years or older can register.	
Singapore	Air Navigation Bill passed 4th Nov 2019	From 2 January 2020 any unmanned aircraft that weighs more than 250g must be registered (sticker with a unique registration number). All registrations to be completed by April 2020.	No requirements yet
Switzerland	FOCA (Federal Office of Civil Aviation) Federal Act on Air Transport and the respective ordinances, as well as the Ordinance on Special Category Aircraft	Currently no registration requirement in Switzerland. No marking system either. Switzerland will implement EU UA Regulations (EU 2019/947) from January 2021 (postponed in line with the rest of Europe. Current Swiss regulations on the operation of UA will remain in force until the end of 2020. https://www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/Europaeische_Drohnenregulierung_uebernommen.html	As part of the Swiss U-Space Implementation Platform (SUSI) FOCA tested the proposed EU rules (Sept 19) and released a document providing an assessment on Remote ID. The Network Remote ID solution proved fully satisfactory. The broadcast solution also worked as expected in the limits currently defined by the standard. The operationalisation of the standard's broadcast portion remains an open question as Bluetooth and Wi-Fi have clear limitations. The demonstration also highlighted the need to better quantify the limitations and the performance of the broadcast solution. https://www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/u-space.html
United Arab Emirates	General Civil Aviation Authority (GCAA)	All UA, regardless of their weight, used by individuals for recreational purposes, shall be registered with the GCAA. Authorisation is required for professional use of UA.	No requirements yet.
United Kingdom	Civil Aviation Authority	Drone Code: Requirement to pass a drone test and register with the CAA. The UK will implement the EU UA regulation by January 2021	No requirements yet.

		(postponed in line with the rest of Europe).	
United States	FAA	UAs weighing between .55 – 55 lbs. must be registered with the FAA and labelled with the registration number.	In December 2019 the FAA published a notice of proposed rule-making (NPRM) on remote identification of UA for public consultation. Proposals allow for both Bluetooth and Wi-Fi remote ID broadcast as well as Network Remote ID. Consultation closed early March. Expectation to have the final rule published by the end of 2020. The NPRM proposes a three year implementation timeframe. There are two categories of Remote ID: 1. Standard Remote ID: UAS would be required to broadcast identification and location information directly from the unmanned aircraft and simultaneously transmit that same information to a Remote ID USS through an internet connection. 2. Limited remote ID: UAS required to transmit information through the internet only, with no broadcast requirements. But unmanned aircraft would be designed to operate no more than 400 feet from the control station.

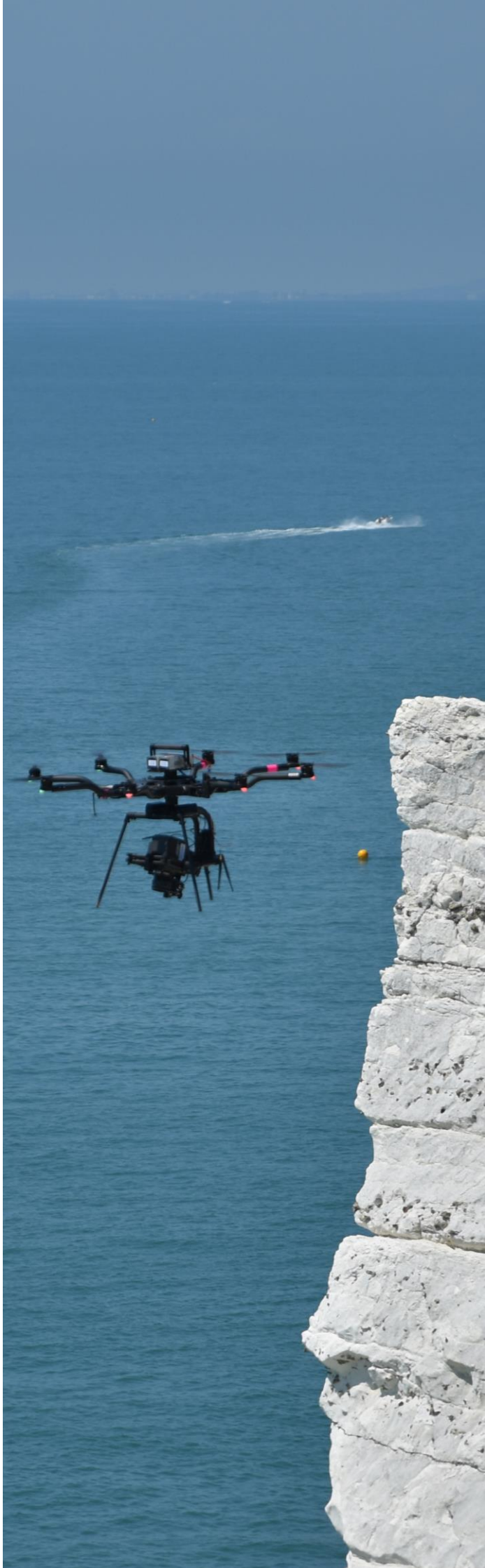
Abbreviations and Acronyms

Abbreviation	Explanation
3GPP	3rd Generation Partnership Project
ADS-B	Automatic Dependent Surveillance-Broadcast
ANSP	Air Navigation Service Provide
APN	Access Point Name
BLOS/BVLOS	Beyond Line of Sight/Beyond Visual Line of Sight
CAAC	Civil Aviation Association of China
CAGR	Compound Annual Growth Rate
CASA	Civil Aviation Safety Authority
D2D	Device to Device
E-CID	Enhanced Cell ID
eNodeB	Evolved Node B
EU	European Union
FAA	Federal Aviation Administration
FLARM	FLARM or flight alarm is a traffic awareness and collision avoidance technology for General Aviation, light aircraft, and UAVUAs
GCS	Ground Control Station

GPRS	General Packet Radio Service
HSPA	High Speed Packet Access
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
LAANC	Low Altitude Authorization and Notification Capability
LCS	Location Services
LOS	Line of Sight
LTE	4G Long Term Evolution
LTE-A	Long Term Evolution Advanced
LTE-M	Long Term Evolution for Machine type
MNO	Mobile Network Operator
NB-IoT	Narrowband IoT
NPRM	Notice of Proposed Rule Making
OTDOA	Observed Time Difference Of Arrival
PDN	Packet Data Network
Remote ID	UAS Remote Identifier
RPIC	Remote Pilot In Command

RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSTD	Reference Signal Time Difference
SIM	Subscriber Identity Model
SMLC	Serving Mobile Location Centre
SSID	Service Set Identifier
SUSI	Swiss U-Space Implementation
TRAFICOM	Finnish Transport and Communications Agency
UA	Unmanned Aircraft
UAOP	Unmanned Aircraft Operator Permit
UAS	Unmanned Aircraft System
UIN	Identification Number
UMTS	Universal Mobile Telecommunications System
UOM	UAS Operation Management System
US	United Sates
USS	UAS Service Supplier
UTM	Unmanned Traffic Management
VLL	Very Low Level

For Further information, visit:
www.gsma.com/aviation



GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com