Utilising Mobile Connectivity for Drones Remote Identification

Wednesday, 15 July 2020 | 10:00 EDT | 15:00 BST | 16:00 CEST
• Don’t forget to submit your questions for the panel discussion

Source: https://support.bluejeans.com/s/article/BlueJeans-Event-instructions-for-Attendees
Polls

• There will be 2 polls during today’s IoT WebTalk

Source: https://support.bluejeans.com/s/article/BlueJeans-Event-instructions-for-Attendees
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 min</td>
<td>Welcome and Introduction</td>
<td>Barbara Pareglio, Executive Director for Aviation and Drones, GSMA Internet of Things</td>
</tr>
<tr>
<td>10 min</td>
<td>Introduction to Remote ID: The Principles, Current Regulations and Future Plans in the USA</td>
<td>Jay Merkle, Executive Director, UAS Integration Office, FAA</td>
</tr>
<tr>
<td>10 min</td>
<td>European Regulations and Future Plans</td>
<td>Natale Di Rubbo, Drone Project Manager, EASA</td>
</tr>
<tr>
<td>10 min</td>
<td>Skyward’s Initiatives (USA)</td>
<td>Eric T. Ringer, Co-founder and Director of Aviation Technology, Skyward, A Verizon company</td>
</tr>
<tr>
<td>10 min</td>
<td>Vodafone’s Initiatives (Europe)</td>
<td>Dr Eric Murray, Principal Engineer, Vodafone Group Technology</td>
</tr>
<tr>
<td>15 min</td>
<td>Interactive Panel</td>
<td>• Jay Merkle. Executive Director, UAS Integration Office, FAA</td>
</tr>
<tr>
<td></td>
<td>Q&amp;A</td>
<td>• Natale Di Rubbo, Drone Project Manager, EASA</td>
</tr>
<tr>
<td></td>
<td>Poll Results</td>
<td>• Eric T. Ringer, Co-founder and Director of Aviation Technology, Skyward</td>
</tr>
<tr>
<td></td>
<td>Closing</td>
<td>• Dr Eric Murray, Principal Engineer, Vodafone</td>
</tr>
</tbody>
</table>

Moderator: Barbara Pareglio, Executive Director for Aviation and Drones, GSMA Internet of Things
Standard Methods of Identification and Registration

Cars
Since 1903-04

Airplanes
Since 1919

Smartphones
Since the late 1990’s
What the GSMA is doing

• The GSMA is actively working with the mobile 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.

• To find out more, visit https://www.gsma.com/iot/connectedskies/
UAS Remote Identification
Jay Merkle, Executive Director
FAA UAS Integration Office

July 15, 2020
1. Every UAS broadcasts a signal that includes a UAS ID (its “license plate”) and operator location
2. Key information is also available through the internet for every operation
3. Authorized individuals can look up UAS ID to find the UAS owner
4. Compliance is easy, and non-compliance stands out clearly
5. Third party USSs build and operate the network infrastructure
Remote ID Pillars

Operating and Production Requirements
(proposed Part 89 Rule)

Remote ID USS Network
(contractcd third party service suppliers)

Industry Standards/Means of Compliance
(standards bodies such as ASTM, others)
UAS Traffic Management (UTM)

Suite of Capabilities:
- LAANC
- Remote ID
- Registration
- Dynamic Airspace

UTM Ecosystem
Natale Di Rubbo

Drone Project Manager

EASA
European Aviation Safety Agency
Remote identification
Direct remote identification

Requirements included in Regulation (EU) 2019/945

Mandatory for UAS with CE class mark C1, C2, C3, C5 and C6

EU States may define geographical zones where only UAS with remote identification can operate
Network remote identification

Required when operating in zones where the U-Space is deployed

Requirements included in Regulation (EU) 2019/945

Optional for UAS with CE class mark C1, C2, C3, C5 and C6
Remote Identification

The Foundation of Universal Traffic Management

- FAA Remote ID cohort member
- Developing means of compliance
- Gateway to drone ops of the future
Cellular in the Air

© 2020 Verizon. This document is the property of Verizon and may not be used, modified or further distributed without Verizon’s written permission.
Network-based Drone Authentication Through APIs

Dr. Eric Murray
Vodafone Group Technology
15 July 2020
EU Regulations on Drone Identification

• What does EU 2019/945 say?
  – Direct remote identification is mandatory (for most classes)
  – Network remote identification is optional

• Vodafone and the GSMA worked to ensure the requirement was technology neutral

• For direct remote identification
  – Original proposed regulation mandated short-range technologies, such as WiFi or Bluetooth
  – Now Cellular D2D (Device to Device) can also satisfy the published regulation
  – This technology is maturing quickly through its use in V2V (Vehicle to Vehicle) use cases

• For network remote identification
  – Cellular is the obvious “network”, but the application data would be transparent to the network
  – It is expected that the requirements will evolve to include U-space, but still under development

Anticipating the evolution of requirements, Vodafone have been working on connecting and authenticating drones to U-space using cellular connectivity
How are Cellular Devices currently Authenticated?

• IMSI (International Mobile Subscriber Identity)
  – The **primary identifier** used for authentication by the cellular network, and very secure
  – Stored in the SIM, and identifies the subscriber (account owner) and not the device
  – **Used internally** by the network for uses such as:
    – billing and quota enforcement
    – associating the subscriber with other identities, such as the MSISDN (the “phone” number)
  – The **device itself can be identified by IMEI**, but this is not securely authenticated

• For voice and SMS, the **MSISDN** is forwarded to the destination to identify the call originator

• But for data services, **no unique identifier for the originator is provided**
  – The source IP address is **NATed using a shared pool**, so not unique to a specific user
  – The IP address, port and time of use can be used to identify the user **retrospectively**, but not in real-time
  – Authentication between client and server is separate from and transparent to the cellular network

Whilst client/server authentication could be used to authenticate drones to U-space, network-based authentication offers important security benefits
How Might the Requirements for Authenticating Drones Differ?

- Not all drone users will be “honest”, and may try to spoof the U-space

- Hence the U-space system would like to be sure that:
  - the connecting device really is a drone
  - it really is operated by who it says it is
  - it really is where it says it is
  - it is connected and remains connected via cellular for the duration of the flight

- All of this information is available to the cellular network independently of the drone
  - The SIM can be registered as a drone SIM
  - The drone IMSI can be used to cross-reference the drone operator identity
  - Network-based geo-location techniques (e.g. Vodafone’s Radio Positioning System) can be used to independently estimate the location of the drone
  - Propagation prediction tools can be used to confirm the proposed flight path has adequate cellular coverage

How can the cellular network provide these additional parameters to the U-space?
Communicating with U-Space via APIs

- The drone communicates with the U-space via an **API Gateway** within Vodafone’s network
  - The API gateway **adds additional identifying information** to the connect request, independently of the drone
  
- The U-space can get additional information using **additional APIs** (e.g. location updates or coverage predictions)
  
- Drone and U-space can exchange information during flight via **API Gateway** (e.g. status updates, flight plan updates)
  
- The API Gateway authenticates the U-space, and can support multiple U-spaces or changing U-space APIs transparently to the drone.
Summary

- Cellular D2D technology is one solution for EU “direct remote identification” requirements
  - This technology is rapidly maturing through its use for Vehicle-to-Vehicle uses cases
- But if the drone is also connected to the cellular network, Vodafone can provide secure verification of the drone’s identity to U-space or other systems
  - The network can also verify parameters such as the drone’s location or predicted coverage quality
- By interfacing through a secure API Gateway, this verification is independent of the drone application, and thus not easily spoofed
  - Equivalent to 2FA, with the second factor provided by Vodafone
- An API Gateway also allows U-space systems to evolve without the need to necessarily update the drone client

Vodafone have a large programme exposing network capabilities through APIs to support novel use cases
Panel Discussion and Q&A

JAY MERKLE
Executive Director,
UAS Integration Office
FAA

NATALE Di RUBBO
Drone Project Manager,
EASA

ERIC RINGER
Co-founder and Director, Aviation Network Technology,
Skyward

Dr ERIC MURRAY
Principal Engineer,
Vodafone Group Network Technology

BARBARA PAREGLIO
Executive Director for Aviation and Drones,
GSMA Internet of Things
GSMA’s Connectivity for Aviation Project

- This IoT WebTalk was recorded and a link to the **On-Demand video** recording will be sent to you within the next few days as well as other relevant materials. These assets will also be posted on [https://www.gsma.com/iot/iot-resources/](https://www.gsma.com/iot/iot-resources/)

- To find out more about our Connectivity for Aviation project, visit [https://www.gsma.com/iot/connectedskies/](https://www.gsma.com/iot/connectedskies/)

- Contact us on [Drones@gsma.com](mailto:Drones@gsma.com)

Thank You!