Gemalto as trust enabler in the drone ecosystem

Drone ecosystem stakeholders

- Providers
- Manufacturers
- Pilots
- Public authorities
- Customers

The first FAA commercial drone regulations took effect in USA on 10 December 2015. This means drones are classed as unmanned aircraft vehicles (UAVs) for the purposes of the Federal Aviation Administration (FAA).

The need for control and regulation

- Public safety
- Civilian and military applications
- Infrastructure development
- Public utilities inspection
- Agriculture
- Construction
- Maritime
- Security

But security isn’t simple

- Near-misses involving drones and manned aircraft by 2020.
- 1,800 sightings of UAVs in the US, pilots of manned aircraft reported.
- First collision in 2017.

Seven key factors for a secure drone ecosystem:

1. Economic and drone registration
2. Protection of sensitive data on the drone
3. Solutions and secure connectivity
4. Reliable drone tracking
5. Protection of flight control commands
6. Confidentiality of data exchange between devices and operators
7. Flight traceability of data

Gemalto as trust enabler

- Secure and seamless connectivity
- Industry leading, high-performance eSIMs
- Built-in firmware so they can be flown
- Protection of flight control commands
- Data is encrypted and stored on secure servers
- Gemalto encryption technology
- Data protection

Public authorities need to ensure citizen safety and law enforcement. Gemalto helps ensure trust at every stage:

- Remote pilot and drone registration through mobile devices
- Seamless and secure connectivity to any cellular, Wi-Fi or internet
- Built-in firmware so they can be flown
- Data protection
- Gemalto encryption technology
- Data protection

Gemalto facilitates worldwide drone networks in all countries.

Currently, some countries have already put commercial drone regulations in place. For example, France, Germany, Spain and the UK.

Some categories of commercial drones will connect via GSM to unmanned aircraft.

Gemalto allows seamless and secure connectivity to any cellular, Wi-Fi or internet.

Remote ID verification via Gemalto’s Cogent biometric technology using remote digital drone ID registration.

Major retailers like Amazon, UPS and DHL are studying the feasibility of using drones for dispatching small packages over short distances.

National and international policymakers are assessing how drones can be used to support emergency operations, so they can quickly firefights, disaster response crews, and law enforcement.

Some drones are designed to be flown by authorized pilots remotely with strong security features.

This data must not be modified. Each drone must also be linked to a digital ID such as serial numbers, and built-in firmware so they can be flown. It includes built-in security features such as geolocation and time stamping are protected from modification.

For easy worldwide deployment, drone manufacturers need their drones to be connected to public authority servers in real time. This data must not be modified.

The need for control and regulation

- Public safety
- Civilian and military applications
- Infrastructure development
- Public utilities inspection
- Agriculture
- Construction
- Maritime
- Security

Gemalto as trust enabler in the drone ecosystem

© Gemalto 2017 - All rights reserved - December 2017 - Wondercorp