

Security Flies High with RIoT Secure's MKR-Based Solution

By The Arduino Pro Team

Arduino's open-source products are at the core of a solid answer to hacking and cyber risk in airports.

The Challenge

Airports clearly give security the utmost importance: stringent rules must be rigidly followed — but also quickly updated as needed, without creating vulnerabilities.

Stockholm-based company RIoT Secure (<http://riotsecure.se>) was founded to address the current and potential security issues our world faces, as billions of objects are connected to the Internet and IoT emerges as one of the strongest growing trends of our time. For them, working with SAS (Scandinavian Airlines) Ground Handling provided the ideal high-constraint project to prove security can be embedded at the core of any IoT solution.

In airports, service vehicles are tracked both for billing purposes and to ensure compliance with safety and security protocols — which constantly evolve. For example, geo-fencing boundaries must be checked in real time to avoid anyone entering forbidden zones, and staff must use RFID-based security badges to access and operate the equipment.

Therefore, in designing a new solution, the critical requirement RIoT Secure was asked to meet was to ensure that all network communications were secure, and that firmware updates could be performed over-the-air, instantly, and across the entire fleet of vehicles.

Our Solution

RIoT Secure developed a secure device lifecycle management platform based on Arduino MKR boards, for communications and over-the-air updates specifically targeting resource-constrained microcontrollers.



RIoT Secure: Secure Device Lifecycle Management with Arduino. Watch it on: <https://youtu.be/RPUGTsawp5E>

The Arduino MKR family was chosen for its modular approach and the capability to offer both Wi-Fi, 3G, and NB-IoT connectivity and a secure element to ensure a root of trust — an excellent foundation for the platform's network freedom.

RIoT Secure rewrote the networking libraries underlying firmware — which utilizes FreeRTOS for multi-threading support — with security-by-design in mind. This allowed them to create a solution that ensures:

- robust and failsafe communication
- long-term device reliability
- freedom to choose the best network topology
- freedom to use the most appropriate microcontroller for each task
- complete isolation from hacker attacks, minimizing security vulnerabilities



Arduino MKR boards.

Finally, while updates are made incredibly simple by using the Arduino IDE and RIoT Secure's lifecycle management platform, the solution's flexibility reaches future-safe levels with the freedom to upgrade or replace the Arduino MKR device as technology evolves, independently of firmware development.

RIoT Secure's lifecycle management platform is licensed to Ingwaz who has the business relationship with SAS ground handling. Ingwaz is a company co-founded by EIT Digital, which supports and spearheads breakthrough technology within digitization for Europe. ◀

220401-01

"SAS Ground Handling can now ensure their equipment are securely connected to the cloud, and that they can enhance the safety and security protocols implemented at the edge in a matter of seconds."

Aaron Ardori, CEO of RIoT Secure



Related Products

- **Arduino MKR Family**
www.elektormagazine.com/arduino-mkr-family