Security Partner Preferred

Partner Use Case

PKI in action - Securing the commercial use of multicopters

PrimeKey

PrimeKey® and Infineon present a solution that enables the safe commercial use of multicopters while being easy to implement. The solution combines Public Key Infrastructure (PKI) with the OPTIGA™ Trust M security controller and the OPTIGA™ Connect IoT eSIM for mobile IoT applications.

Products

OPTIGA™ Trust M & OPTIGA™ Connect IoT

Use case

Application context and security requirement
Almost half a million multicopters are currently in service in Germany. The majority are used privately, but the unmanned vehicles are more than just a gimmick. According to a study by the German Unmanned Aviation Association (VUL), professional use will increase significantly up until 2030. By then, every sixth multicopter will be operated commercially. Because of its diverse uses, the technology has great potential for organizations. For example, multicopters simplify the inspection of construction projects, buildings or infrastructures such as wind turbines and high-voltage lines. They can also facilitate terrain surveying, help with mapping tasks or take photographs and film shots from the air. The study by VUL showed that from 2026, multicopters will be used throughout the country in the main commercial areas of application.

In certain multicopter use case scenarios, it is important that the aircraft can be uniquely identified and authenticated – for example, if it is deployed near no-fly zones. It is also crucial for air traffic control to be able to intervene in an emergency.

Challenge
Like many new technologies, unmanned aerial vehicles also entail certain risks. For example, flight operations have already been disrupted several times because of intruding multicopters. Frankfurt Airport had to be completely shut down for a short time in May 2019 and London-Gatwick was out of action for several days in December 2018. Additionally, multicopters are becoming increasingly attractive as targets for cyber criminals who can capture them and steer them into no-fly zones.
To contain such dangers, multicopters must be properly secured for commercial use.

Implementation
In order to provide comprehensive safety, multicopters must be clearly identifiable and simultaneously meet the requirements for the control system. This protects them from manipulation and hinders unauthorized users from taking over the control system. In addition, authorized control instances and commercial operators should be able to monitor the multicopter via GPS (Global Positioning System) and intervene in the event of danger. In some commercial scenarios, it may be necessary to enter no-fly zones with a special permit, for example when inspecting a critical infrastructure facility or a government building. For this purpose, multicopters must also be securely identified and authenticated.
In a joint pilot project, PrimeKey and Infineon have shown how these challenges can be met. The solution enables companies to make full use of multicopters while minimizing security risks. Infineon contributes its expertise as a manufacturer of security controllers. PrimeKey, one of the world's leading PKI providers, contributes its know-how in the field of public key infrastructure management. The project was developed in the Infineon Security Partner Network (ISPN), in which Infineon develops end-to-end security for Internet of Things (IoT) applications with various partners.

User benefits
"Multicopters present a variety of security challenges, including
› the need to protect against manipulation,
› clearly authenticate each device
› and activate an intervention in the event of a safety risk.

The Infineon Security Partner Network demonstrates how matching competencies can be combined to generate a higher customer value. PrimeKey's public key infrastructure management expertise is the perfect complement to Infineon's market-leading hardware security solutions. The result is an end-to-end solution that unleashes the full potential of multi- copters without compromising on safety or security."
– **Cristina de Lera**, Senior Director of Infrastructure and Device Security, Infineon Technologies

Solution

The multicopter security solution consists of the following components:

PKI service

With the help of the PKI, the multicopter is securely identified and authenticated. This is achieved on the basis of a certificate containing the aircraft's identification data and an electronic signature meaning that the identity of the multicopter is protected from being forged by other users. Other parties, such as flight supervisors, can also be a diagram representing the solution and/or the operational flow included in the PKI hierarchy via a certificate, establishing a relationship of trust between the systems while PrimeKey provides the PKI as a managed service from a German data center. This means that customers do not have to take care of the setup and operation themselves and do not need PKI expertise.

OPTIGA™ Trust M

OPTIGA™ Trust M is Infineon Technologies' embedded connected security solution for the complex integrated requirements for today's and future security demands of multicopter ownership and operations. The Trust M with Infineon personalized certificates and Elliptic Curve Cryptography (ECC) generates the cryptographic key pair consisting of a private key and a public key and stores it securely along with further keys, PKI etc. within a tamper-resistant EAL6+ hardware solution. Furthermore, the powerful OPTIGA™ Trust M enables an easy to use cryptographic toolbox for highly flexible customization along with on-chip cloud connectivity via Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS).

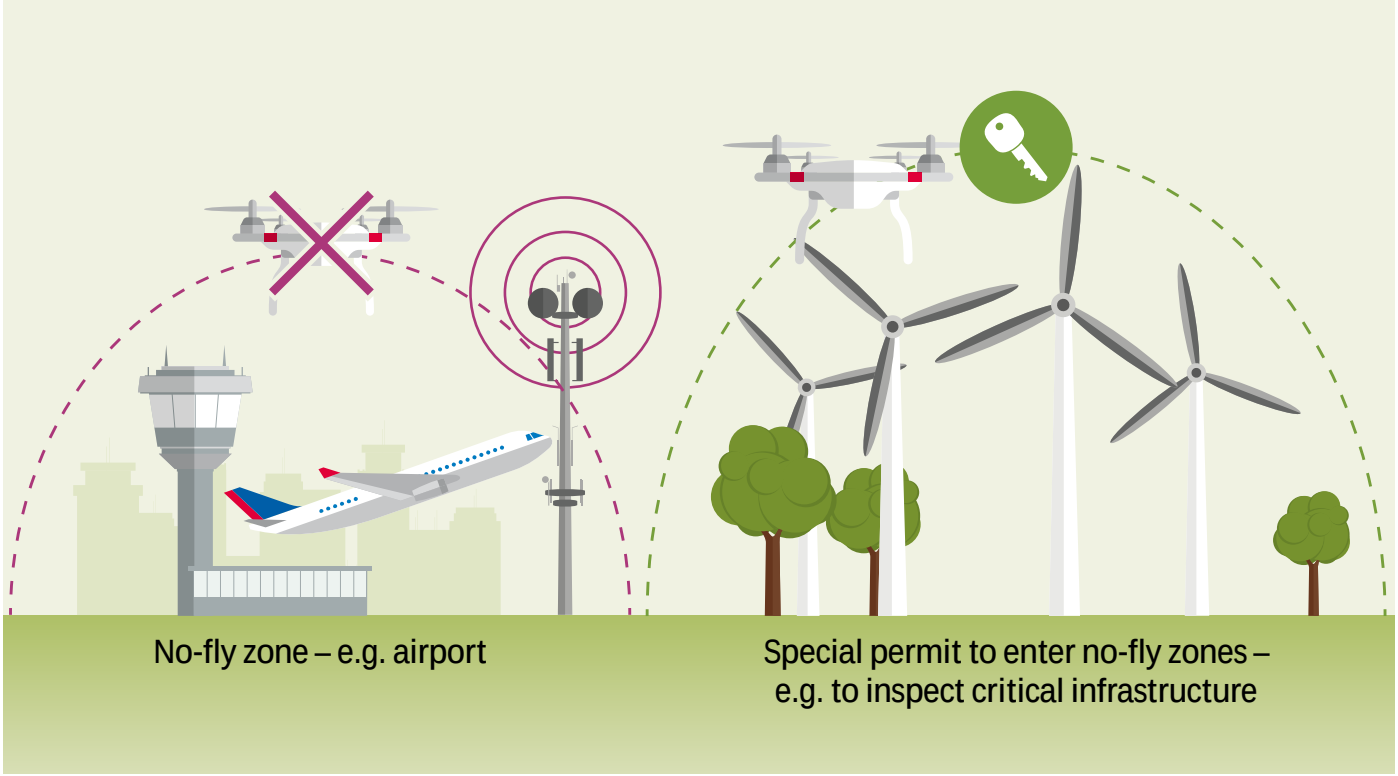
OPTIGA™ Connect IoT

The OPTIGA™ Connect IoT is M2M (Machine-to-Machine) GSMA (Groupe Speciale Mobile Association) certified and allows to authenticate against 2, 3, 4G or LTE networks. This provides reliable connectivity for the multicopter. Infineon's eSIM technology enables multiple use cases – for example, the global deployment with single device design. That means one 'stock keeping unit', where the connectivity can be selected according to where the device is activated. The other option is the dynamic selection of a network operator provider to ensure continuity and quality of connectivity. This also makes the eSIM suitable for more advanced use cases in which the mobile network is selected according to the geolocation of the device via GPS. PrimeKey and Infineon developed an easy-to-integrate solution that requires little know-how on the basis of a Raspberry Pi and put it into operation within half a day. Raspberry Pi Shields are available for the OPTIGA™ Trust M as well as the OPTIGA™ Connect IoT and can be put to use immediately. For testing the interaction with the PKI service, PrimeKey offers its open-source EJBCA® Enterprise software.

Solution

In practice: How multicopters can be used securely at the airport

In our chosen scenarios, the multicopter cannot enter into no-fly zones unless correct permission is explicitly provisioned. The OPTIGA™ Trust M security solution is providing secured multi-certification and key handling.
In practice, it looks like this: the multicopter pilot logs into the system with his credentials and triggers the PKI process. The cryptographic key pair consisting of a private and public key is securely generated by the OPTIGA™ Trust M toolbox. The OPTIGA™ Trust M then sends the public key within a Certificate Signing Request (a request to create a certificate) via the mobile network to the PKI service. The OPTIGA™ Connect IoT sets up a stable LTE connection via the chosen Mobile Network Operator (MNO) provider. The PKI identifies the requestor, provides the certificate and sends it back to the multicopter, where the OPTIGA™ Trust M stores it within the EAL6+ tamper-resistant hardware platform. After the certificate installation, the multicopter is included in the PKI hierarchy. The remote control is activated, and the pilot can start the multicopter. A control instance can also be incorporated into the PKI hierarchy via a certificate. It can communicate with the unmanned aircraft and monitor its position using GPS data. If the multicopter enters an unauthorized area, the control instance can take over and land the aircraft safely at the touch of a button.



Main benefits of the Infineon products

The OPTIGA™ Trust M is a high-end security solution that provides an anchor of trust for connecting IoT devices to the cloud, giving every IoT device its own unique identity. This pre-personalized turnkey solution offers secured, zero-touch onboarding and the high performance needed for quick cloud access.

OPTIGA™ Trust M offers a wide range of security features, making it ideal for industrial and building automation applications, smart homes and connected consumer devices.

The turnkey set-up with full system integration minimizes design, integration and deployment effort.

Solution

OPTIGA™ Connect IoT is a ready-to-connect embedded SIM (eSIM) solution for cellular IoT devices. This turnkey solution allows easy, secured and cost-optimized deployment and management of cellular-enabled IoT devices at scale. It comes with a pre-installed GSMA-compliant operating system and pre-integrated connectivity capabilities. Supported by our partner Tata Communications, OPTIGA™ Connect IoT offers global cellular network coverage (2G, 3G, 4G, CATM and other LTE services) spanning 640+ networks across 200 countries.

End-to-end connectivity management extending from design through manufacture to deployment reduces complexity, offers full visibility into IoT devices and simplifies control. It addresses today's key pain points in connectivity management, namely interoperability, technical support, cost, and coverage.

OPTIGA™ Connect IoT is based on Infineon's best-in-class Common Criteria EAL5+ certified eSIM hardware, which is designed to exceed the security standards typically required by industry today. This adds an additional level of tamper resistance to these solutions, hardening them against physical attacks – which is especially important for devices that remain in the field for long periods of time.

Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

PrimeKey Solution AB

One of the world's leading companies for PKI solutions, PrimeKey has developed successful technologies, such as EJBCA® Enterprise, SignServer Enterprise and PrimeKey® EJBCA Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organizations around the world with the ability to implement security solutions, such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation.

PrimeKey's contribution to the Infineon Security Partner Network

PrimeKey® delivers the enabling PKI and Digital Signature technology to leverage Infineon's security solutions. By supporting a variety of different Infineon OPTIGA™ products for securing encryption keys and the process of issuing digital certificates, together we can offer a joint solution targeting various vertical markets. Especially in the broad application area of IIoT/IoT, the joint offering of Infineon OPTIGA™ products in combination with Primkey EJBCA® products provides turnkey solutions to implement trusted communication and device security.

PrimeKey has also added a broad portfolio of PKI and digital signature products to enable industrial security on the manufacturing floor or combined with cloud based PKI and signing solutions, depending on the business context and need.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 12 / 2020

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!

This Document is for information purposes only and any information given herein shall in no event be regarded as a warranty, guarantee or description of any functionality, conditions and/or quality of our products or any suitability for a particular purpose. With regard to the technical specifications of our products, we kindly ask you to refer to the relevant product data sheets provided by us. Our customers and their technical departments are required to evaluate the suitability of our products for the intended application.

We reserve the right to change this document and/or the information given herein at any time.

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.