PKI in Action

Securing the commercial use of multicopters

www.infineon.com

PrimeKey

www.primekey.com

Infineon

Abstract

From 2026, multicopters will be widely used in all major commercial applications[1]. Their uses in business and in the public sector is manifold: multicopters can perform surveying tasks or help inspect wind turbines and high-voltage power lines. In such 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. Finally, it is essential to protect the multicopter from being taken over by a third party. In a pilot project, PrimeKey and Infineon presented a solution that enables the safe commercial use of multicopters while being easy to implement. It combines Public Key Infrastructure (PKI) with the OPTIGA™ Trust M security controller and the OPTIGA™ Connect OC2321 eSIM for mobile IoT applications.

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.

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[2] and London-Gatwick was out of action for several days in December 2018[3]. Additionally, multicopters are becoming increasingly attractive as targets for cyber criminals who can capture them and steer them into no-fly zones or in the worst-case scenario misuse them for an act of terrorism. To contain such dangers, multicopters must be properly secured for commercial use.

[1] https://www.bdl.aero/wp-content/uploads/2019/02/VUL-Markststudie_Deutsch_final.pdf
[2] https://www.spiegel.de/wissenschaft/technik/frankfurt-am-main-drohnen-bedrohen-zunehmend-den-flugverkehr-a-1266541.html
[3] https://www.spiegel.de/reise/aktuell/flughafen-london-gatwick-nach-berichten-ueber-drohnen-ist-betrieb-lahmgelegt-a-1244709.html

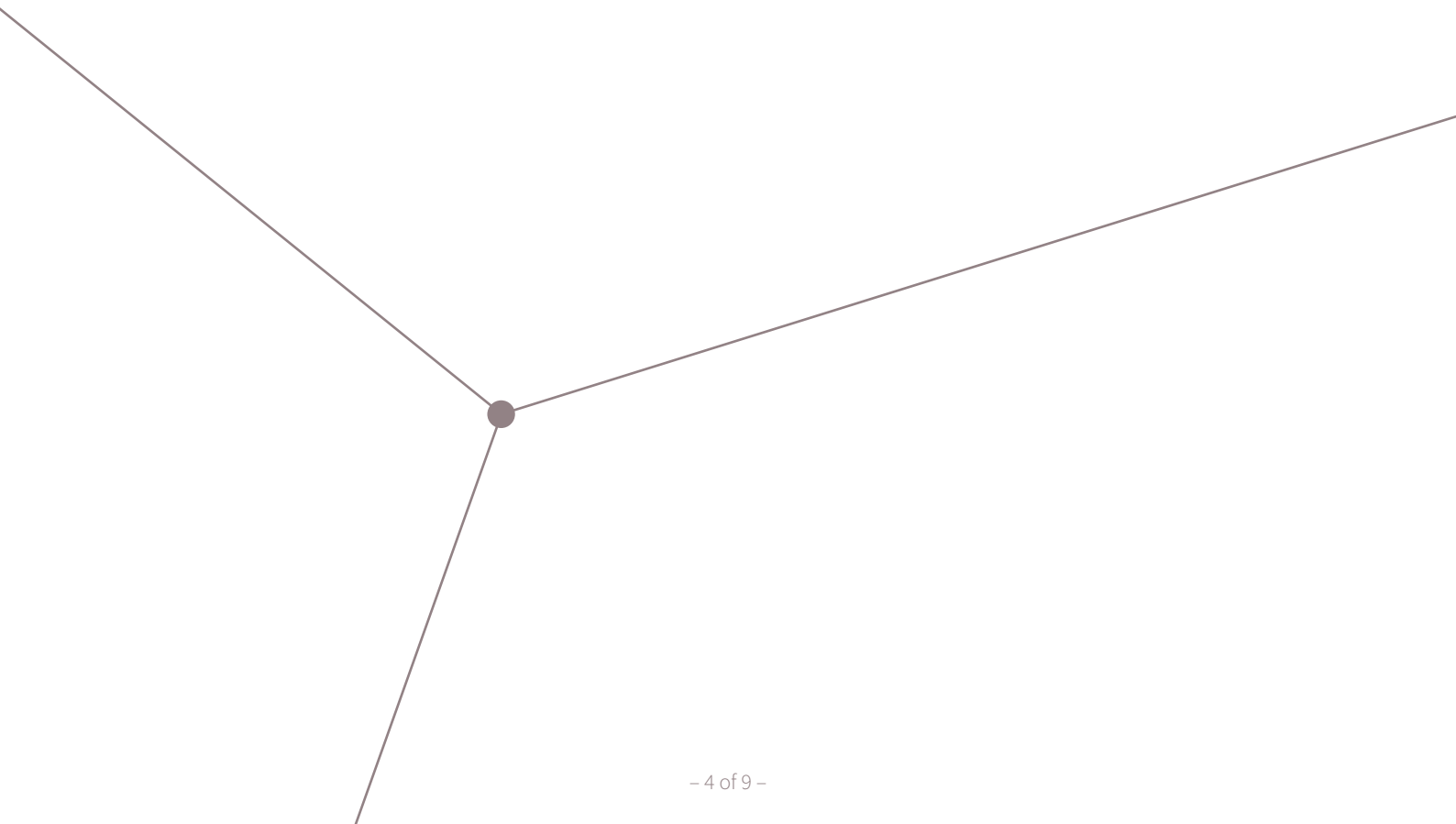
Contents

1. Joint project of PrimeKey and Infineon

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 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.

"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 multicopters without compromising on safety or security."

Cristina de Lera, Senior Director of Infrastructure and Device Security, Infineon Technologies



2. The multicopter security solution consists of the following components:

2.1 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 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.

2.2 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).

2.3 OPTIGA™ Connect OC2321 eSIM

The OPTIGA™ Connect OC2321 eSIM for IoT is M2M GSMA certified and allows to authenticate against 2, 3, 4G or LTE networks. This provides reliable connectivity for the multicopter. Infineon 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 devices 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.

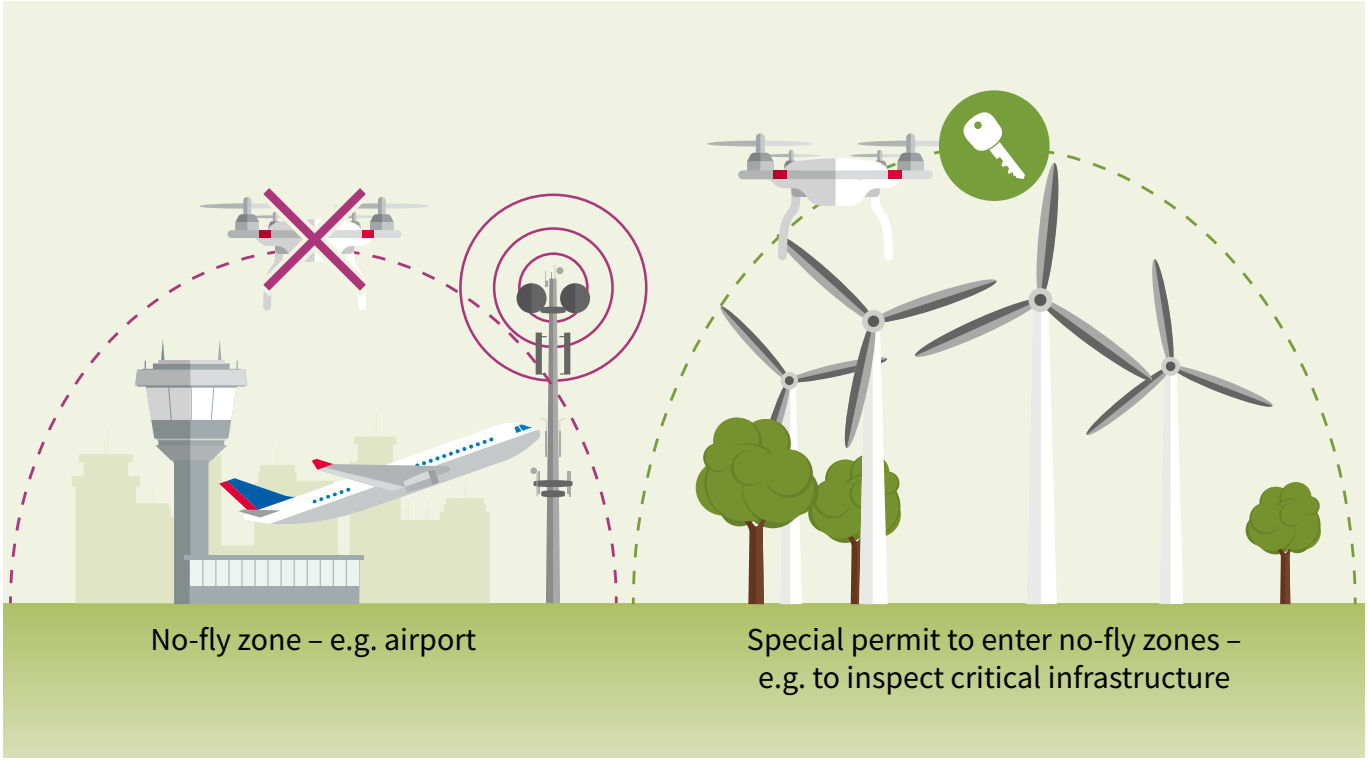
PrimeKey and Infineon developed an easy-to-integrate solution that requires little know-how on the basis of a Raspberry Pi and put it into operation within half a day. Raspberry Pi Shields are available for the OPTIGA™ Trust M as well as the OC2321 eSIM and can be put to use immediately. For testing the interaction with the PKI service, PrimeKey offers its open-source EJBCA software.

3. In practice: secure multicopter deployment 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 OC2321 eSIM 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.



4. A wide range of applications

The multicopter security solution is suitable for all scenarios in which an unmanned aircraft must be certified and authenticated before take-off and in which a supervisory authority needs to be involved. For example, this is the case in no-fly zones that can only be entered with a special permit. As well as airports, flight restrictions also apply to buildings of the highest governmental institutions, military installations and prisons. Multicopters may only fly over industrial facilities with the permission of the owner, as there is a risk of industrial espionage[4]. Operators of critical infrastructures, such as energy and water utilities, are subject to particularly strict security regulations because of their crucial role in public interest. They must therefore keep a precise record of which multicopters have access to their premises and are responsible for analyzing the data collected.

With the security solution by PrimeKey and Infineon, service providers can give their customers secured multicopters for operations such as site monitoring or deficiencies/corrosion checks on bridges. The PKI service issues corresponding certificates, which contain authorizations and regulate the activation. If, for example, a multicopter is to inspect a wind turbine, the certificate is valid for a specified period. At the end of the period, the certificate is deleted again and the multicopter is ready for use by another customer or for a different scenario.

5. Prepared for future regulations

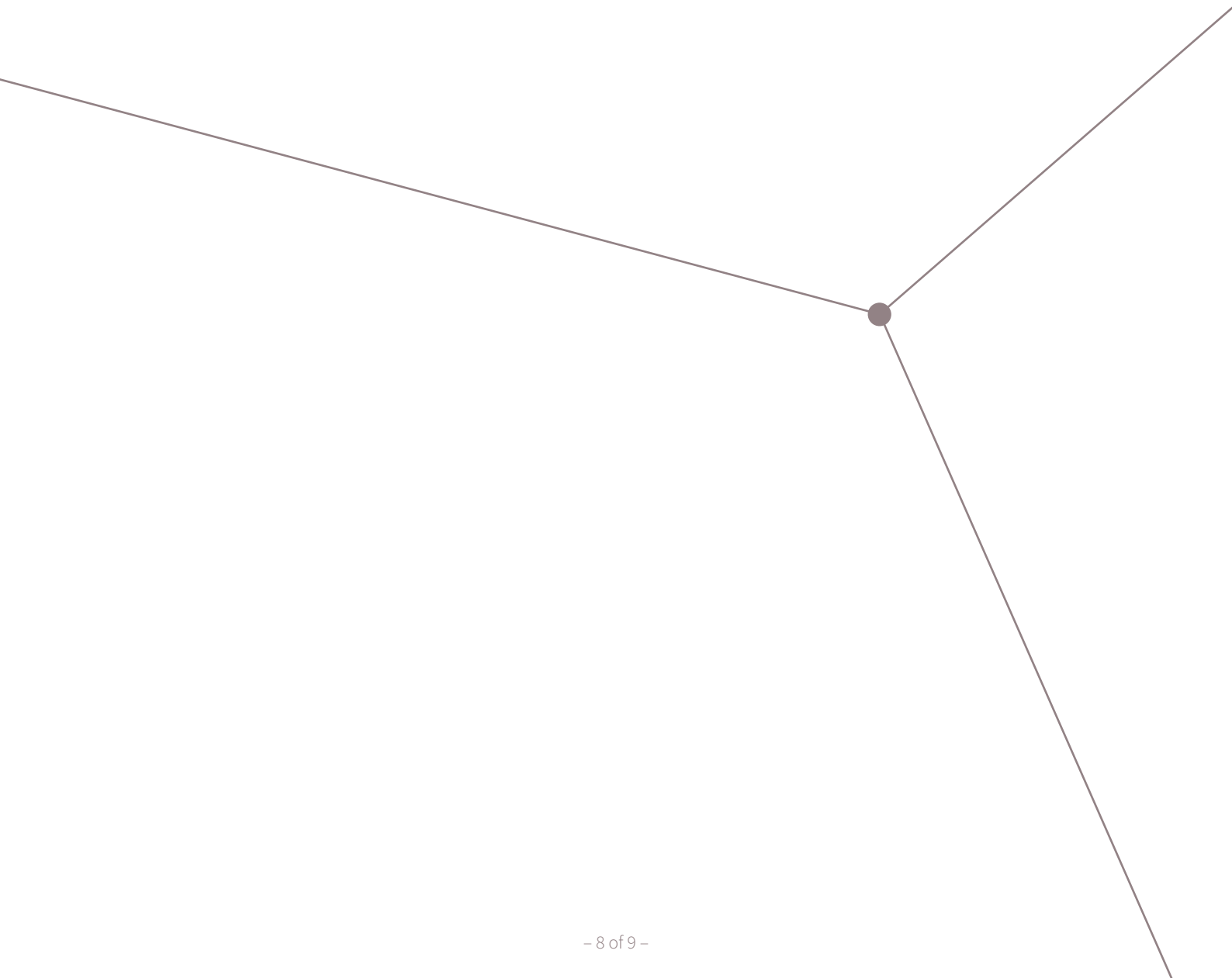
The use of multicopters in no-fly zones is a sensitive issue. Various institutions are currently developing concepts for a more secure airspace. The European Aviation Safety Agency (EASA), for example, wants to make it compulsory for all multicopters to have an LTE connection and a certificate issued by a government institution. The German air traffic control company Deutsche Flugsicherung is currently working on pilot projects with Deutsche Telekom and Vodafone to monitor multicopters via an LTE connection. The worldwide industry association of GSM mobile phone providers GSMA is another organization looking for a practical approach. There are also proposals from the ISO (International Organization for Standardization). However, no binding, uniform regulation has been found meaning multicopter manufacturers are still hesitant to integrate security solutions into their aircraft. PrimeKey and Infineon are submitting various proposals to the GSMA and ISO to speed up the process. With their security solution, they are already prepared for future regulations.

> “A certificate hierarchy is an effective way to secure the commercial use of multicopters. There are efforts to build a worldwide network of trusted authorities that issue certificates to fly multicopters – similar to SSL certificates for browsers. With such a framework, there would be no limits to multicopter use cases.”
>
> Andreas Philipp, Business Development Manager at PrimeKey

[4] https://www.bvzd.org/themen

6. Conclusion/Outlook

Multicopters have great potential for the international economy. In order for companies to tap into this potential, however, the commercial use of unmanned aerial vehicles must be secured. In their joint pilot project, PrimeKey and Infineon presented a possible solution that combines embedded security with a security controller, LTE communication via the OPTIGA™ Connect OC2321 eSIM as well as public key infrastructure. If multicopters are uniquely identified and authenticated in a PKI, misuse can be avoided. Certificates regulate authorization and control instances such as flight control have the option of bringing intruding objects to the ground. Equipped in this way, multicopters will be able to take off securely in the future.



Where to buy

Infineon distribution partners and sales offices:
www.infineon.com/WhereToBuy

Service hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

- Germany ..... 0800 951 951 951 (German/English)
- China, mainland ..... 4001 200 951 (Mandarin/English)
- India ..... 000 800 4402 951 (English)
- USA ..... 1-866 951 9519 (English/German)
- Other countries ..... 00* 800 951 951 951 (English/German)
- Direct access ..... +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number.
Please visit www.infineon.com/service for your country!

Mobile product catalog

Mobile app for iOS and Android.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05/2020

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.

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).

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.