Designing trust into wireless charging applications

http://www.infineon.com/OPTIGA-Trust-Charge

Overview

The Wireless Power Consortium (WPC) Qi 1.3 specification which will be released soon, will include strong cryptographic authentication for wireless charging devices. The new requirement requires that products can prove they have Qi certification, showing they comply with WPC usage and safety standards. This provides peace of mind to consumers and a real benefit to the wireless power ecosystem by allowing that any certified wireless power device can be identified and trusted for safe and reliable charging. Understanding how the Qi spec has employed authentication is important. However, understanding how to securely implement this in a product is even more critical, in order to fully take advantage of the intended protections.

Contents

The need for strong authentication

Wireless charging significantly improves the convenience of electronic devices. The requirement to periodically plug in a device has always been a hassle for the consumer. This problem is multiplied by more electronics, and compounded even further by the need to carry around charging cables and backup battery packs when away from home. The ability to seamlessly charge a device while it is resting on a nightstand in the evening or when sitting in a coffee shop is a tremendous leap forward in usability. The consumer no longer needs to think about charging their device – they can simply focus on using it. However, the greatest concern by far that people have with wireless charging is safety. This is a truly valid concern. Poorly implemented wireless charging can lead to damaged devices and potentially serious injury to the user.

One major area of concern is foreign object detection (FOD). Objects that are not properly shielded can be heated by the magnetic fields on the surface of a wireless power transmitter. For example, in a poorly designed system, house keys that are sitting next to a cell phone on the charge pad could heat up to the point of burning anyone who tries to pick them up. The WPC addresses this potential problem in both the Qi spec and in certification testing.

The Qi spec defines a communications protocol between the transmitter and receiver so the transmitter can correctly identify devices that are Qi compliant and therefore have the necessary shielding to prevent overheating. The transmitter is then able to adjust the field as necessary to avoid heating up any objects that do not correctly identify themselves. This correct identification is important, because it validates that the device knows the correct communications protocol and has proven it can safely handle the delivered power.

Qi certification testing further provides safety by directly testing the transmitter with foreign-object scenarios. These tests confirm that the transmitter can correctly handle unknown objects in a safe manner. Correctly authenticating that the transmitter has a legitimate Qi certification confirms that it has gone through this third-party safety validation and so can be trusted to operate safely.

Interoperability is another major area of concern. The Qi spec defines the communications protocol between the transmitter and receiver to correctly negotiate the power transfer. This can also be a potential safety concern, because an error in this communication could lead to too much attempted power transfer. Confirming that devices are Qi certified enables devices to more confidently connect to third-party wireless charging stations, and in turn enables a thriving ecosystem.

There are also direct benefits to device manufacturers. Beyond just confirming Qi certification, strong cryptographic authentication is widely used today to stop counterfeits and clones. The Qi authentication standard not only confirms that the device has met Qi compliance, but also enables manufacturers to confirm that devices sold under their brand are genuine. This traceability, from WPC certification to device manufacturer to distribution channel or product SKU, can be used to confirm that only legitimate devices are sold, potentially saving the manufacturer significant money in lost revenue.

Finally, Qi authentication benefits the ecosystem as a whole. The ability to confirm Qi certification through strong authentication increases the value of that certification, making the entire wireless charging ecosystem healthier. Companies that invest in proper product development and certification are more likely to reap returns, as their devices are recognized for their quality. This can lead to an increase in interconnectivity and faster market adoption of wireless charging.

Overall, adding cryptographic-based authentication to wireless charging products benefits everyone and enables a safe, reliable and convenient means of charging electronic devices.

Overview of PKI and Qi authentication requirements

With version 1.3 of the Qi spec, the WPC has implemented an authentication scheme using a public key infrastructure (PKI). This type of authentication is used extensively in computer networks and secure device authentication because it is both cryptographically secure and extremely flexible. A single public key can be used to validate the identity of any legitimate device within the PKI system.

PKI relies on asymmetric cryptography, such as elliptic curve cryptography (ECC). In this cryptographic scheme, two keys are used – a private key and a public key. These two keys are different but mathematically linked such that what one key encrypts, the other can decrypt. This has a major advantage for authentication over symmetric cryptography such as AES. With AES, the same key must be used on both sides of the communication. However, with ECC, only the private key must be kept secret, while the public key can be freely shared.

The overall PKI framework is then based on certificates, which are created and signed by a certificate authority (CA). The certificate is created to include public key and other identifying information about the device, such as the device's serial number, the issuer of the certificate, and what kind of certificate it is. The CA then makes a hash digest of the certificate using a SHA-256 algorithm and signs this digest with a CA private key (see Figure 1). Every certificate will have a unique signature, because the hash of the certificate is unique. More importantly, only someone with the correct CA private key can create the correct signature. Therefore, both the private key and the manufacturing steps that sign it must be properly secured.

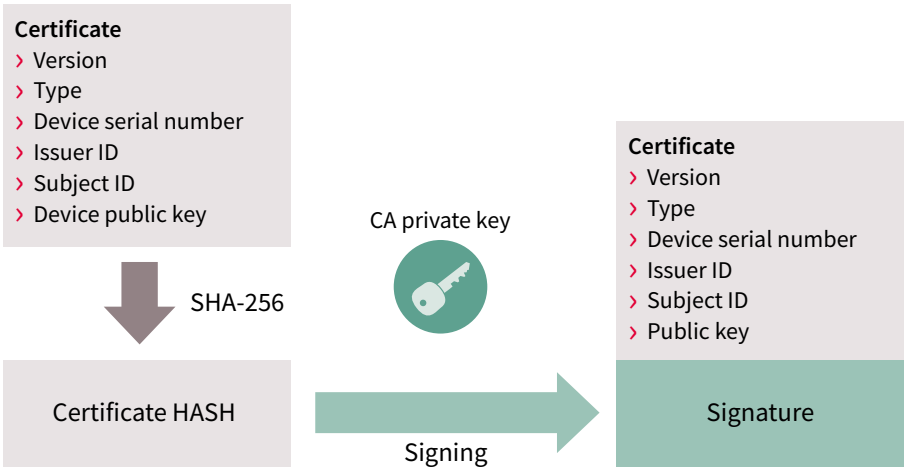

Figure 1: ECDSA signing process

This certificate can then be verified using the public key, which does not need to be kept confidential. The verifier first makes a SHA-256 hash of the certificate. They then use the public key to verify that the signature decrypts to the same hash, which was calculated with the certificate (see Figure 2). If these two digests match, the certificate would be accepted as genuine and the data included in it can be trusted.

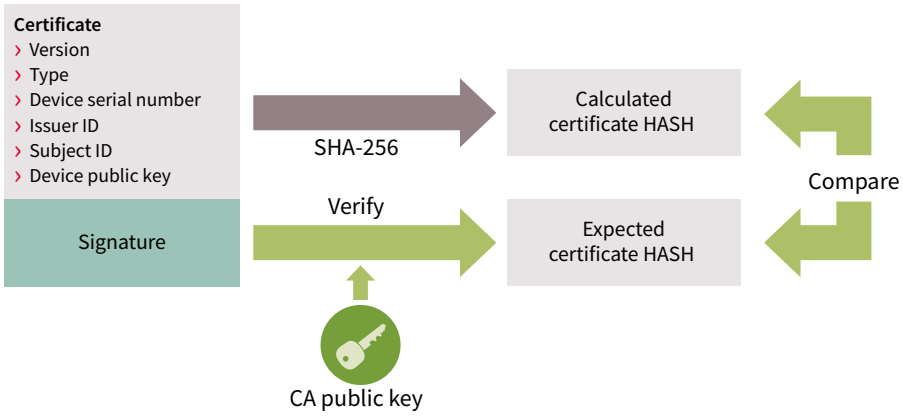

Figure 2: ECDSA verification

Once the certificate has been verified, the device requesting authentication and the device being authenticated enter a challenge–response communication (see Figure 3). During this step, the requesting device sends a "challenge" to the unknown device in the form of a randomly generated number. The responder signs this random number with its product unit private key. The challenger verifies this response using the product unit public key, which was included in the certificate. This provides a method of confirming identity with a unique communication each time, protecting from replay attacks. Only a device with the correct product unit private key creates a response to the challenge, which can be verified with the associated public key in the device's certificate. It is therefore also critical that this private key be kept protected.

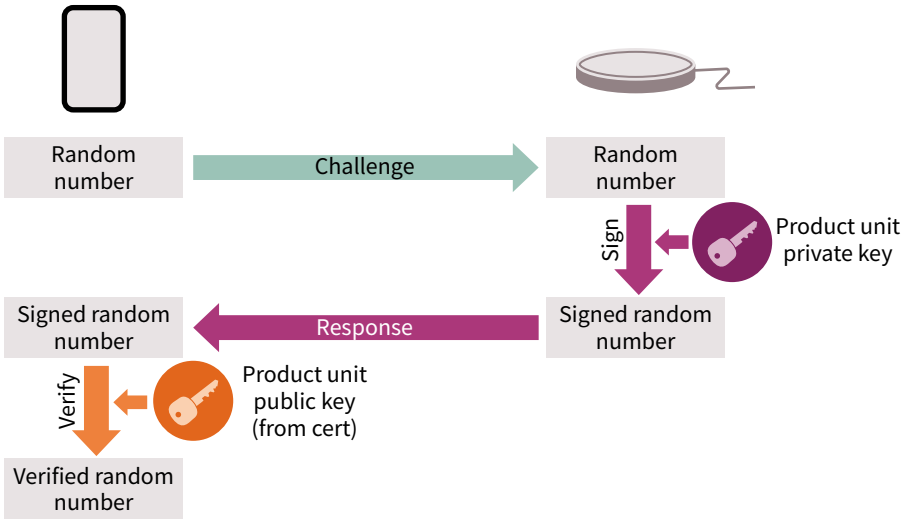

Figure 3: Challenge–response process

This system of certificate verification and challenge–response provides a powerful method of authentication, because each device is loaded with a unique certificate and private key but can be verified as authentic with a single CA public key. Because this public key does not need to be confidential, it can be freely shared with any device that would need to perform the authentication.
This authentication scheme is made even more flexible by certificate chaining.

Chaining certificates is a way to introduce multiple levels of CAs into the authentication system. The root CA has a private key that it uses to sign itself and to sign the next certificate in the chain. The second private key can then sign the third certificate, and so on. Verification becomes easy because the certificates include their own public keys. The second certificate is validated by the root CA public key. The now-validated second public key can then be used to validate the third certificate. The public key from the last certificate in the chain can then be used for the challenge–response.

Version 1.3 of the Qi spec allows for up to four certificates in a chain, which can be used to differentiate by manufacturer, product and an optional intermediate level (see Figure 4). The WPC root CA will sign all manufacturers' certificates, enabling secured access to any valid manufacturer public key. Each company with a Qi-certified product can then sign its own product certificates. An optional secondary certificate slot provides manufacturers with additional flexibility to add another layer of CA, which could differentiate by region, contract manufacturer, product type or any other category they wish. The last layer is the product unit certificate, which provides the unique authentication for a given unit of a product. Overall, this method allows manufacturers to maintain ownership of their private keys and security framework while still only needing to pre-load the WPC root public key into any Qi-compliant device.

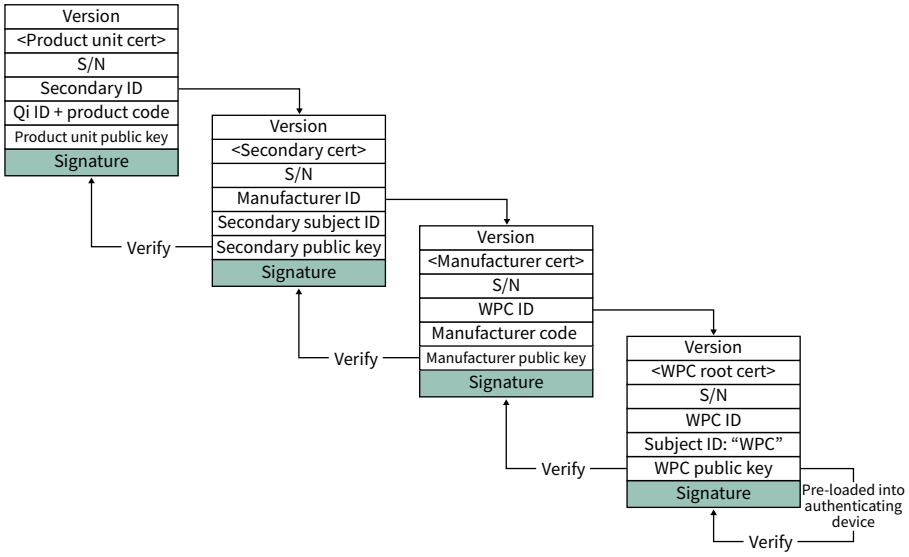

Figure 4: Qi spec v1.3 certificate chain

The Qi spec requires that the first two certificates, the WPC root certificate and the manufacturer's certificate, are formatted in compliance with the Qi spec. However, the optional secondary certificate and the product unit certificate can be formatted as the manufacturer desires. The result is that all Qi-certified devices will be loaded with the following information:

Receivers include:

› WPC root CA certificate hash
› WPC root CA public key

Transmitters include:

› Manufacturer certificate
› Secondary certificate (optional)
› Product unit certificate
› Product unit private key

With this information, the receiver is able to verify the authenticity of any Qi-certified transmitter.

Implementing secured authentication for Qi devices

Understanding the mechanics of how the WPC specifies the authentication protocol is only the first step in securing the device. Implementing this in a product requires an understanding of how devices can be broken and authentication schemes subverted by attackers. Someone who wishes to counterfeit a product or otherwise falsely claim their device is certified needs to gain access to the private keys used to sign the certificates and challenges. They will do this by attacking the weakest part of the system. This might include attacking the product itself, getting access to development records or taking keys from a manufacturing site where the device is provisioned. Protecting the private keys from all possible attacks is vital in order to make the authentication process effective. The WPC states that private keys and certificates must be securely stored. So what does this mean, and how is this done?

The most obvious place to look is the product itself. There are multiple ways an attacker can gain access to data stored in a device's memory (see Figure 5). One attack category is fault attacks. These are aimed at putting the processor in an out-of-spec condition, causing it to glitch and output data from memory. Fault attacks can include voltage, temperature, light and radiation spikes that the processor was never designed to encounter. Another category is side-channel attacks. With these attacks, the adversary measures device characteristics while it is under operation, such as minor variations in power and timing. By this, an attacker could infer the keys used by an unprotected device during the authentication process. A third category is probing attacks. These directly monitor internal signal lines of a decapped IC to record secure data while it is being processed. A different category is reverse engineering, where the counterfeiter analyzes the IC to gain access to physical information on the chip and then attempts to completely replicate it.

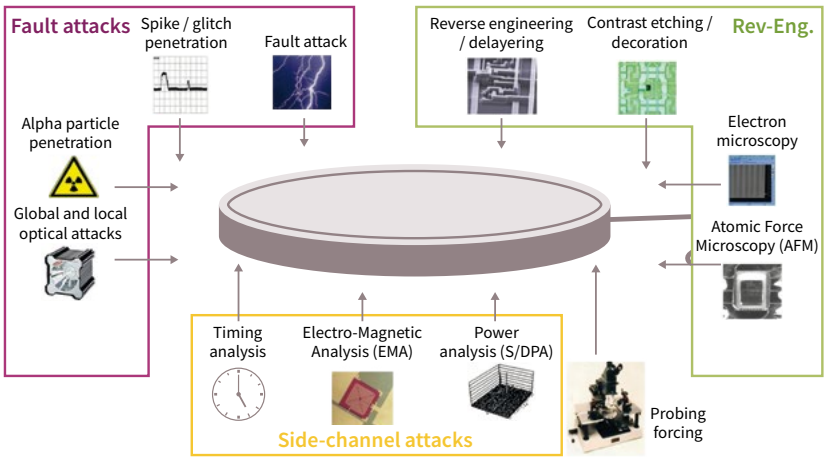

Figure 5: Types of physical attacks

Most processors are not designed to avoid any of these types of attacks. Even processors with built-in cryptoaccelerators or operating environments are not necessarily protected against the types of physical attacks used by counterfeiters. This is where certification bodies can help. They provide an independent evaluation of a product's ability to counter various threats. Common Criteria is one of the most widely used certification standards. Common Criteria test labs evaluate the product itself through penetration testing, product analysis and documentation, as well as judging the security of the design and the manufacturing environment in which it is produced. Common Criteria uses Evaluation Assurance Levels (EALs), where an EAL1 device is just functionally tested while an EAL7 device has undergone a highly rigorous process of evaluation and testing to a strict security standard. Plus symbols are used after the EAL number to denote that specific additional security standards have been met beyond the minimum needed for the given level. Infineon recommends at least EAL4+ certification on the hardware that stores keys and certificates. For that the protection profiles PP0035 and PP0084 could be used as part of the evaluation. These details are still under discussion at WPC. Use of these profiles mean the product is considered security level "high" by Common Criteria, meaning that countermeasures against physical attacks must be included. This gives assurance that the security information can be efficiently protected from the most common attacks.

If the keys are well protected on the product itself, the attacker must look for other places to steal the private keys. The manufacturing locations where devices are programmed and tested are often the easiest targets. These can be subjected to remote network attacks, social engineering attacks on employees or intentional theft by factory personnel. Protecting keys at the manufacturing site involves protecting both the stored keys and the process of provisioning devices. A certified hardware security module (HSM) is needed, along with strict processes around access control and management of the programming steps. Infineon recommends an EAL4+ certification for this step as well. For a manufacturer, this means a thorough security setup and external audits of the provisioning process to evaluate its security effectiveness. Setting up and maintaining a certified manufacturing site is challenging and expensive, so this is often outsourced to security companies that specialize in CA services.

Best-practice example

Overall, implementing effective product security from scratch can be challenging for a company that does not specialize in security products. Developing hardware that can cover the wide range of threats and pass security certification takes time and detailed security knowledge. Setting up the processes in development and manufacturing to effectively protect against attacks is time-consuming and expensive. Fortunately, there are cost-effective solutions on the market that enable fast development time and result in a highly secure device. The best solution is one that incorporates a separate secure element to handle the key storage and authentication protocol (see Figure 6).

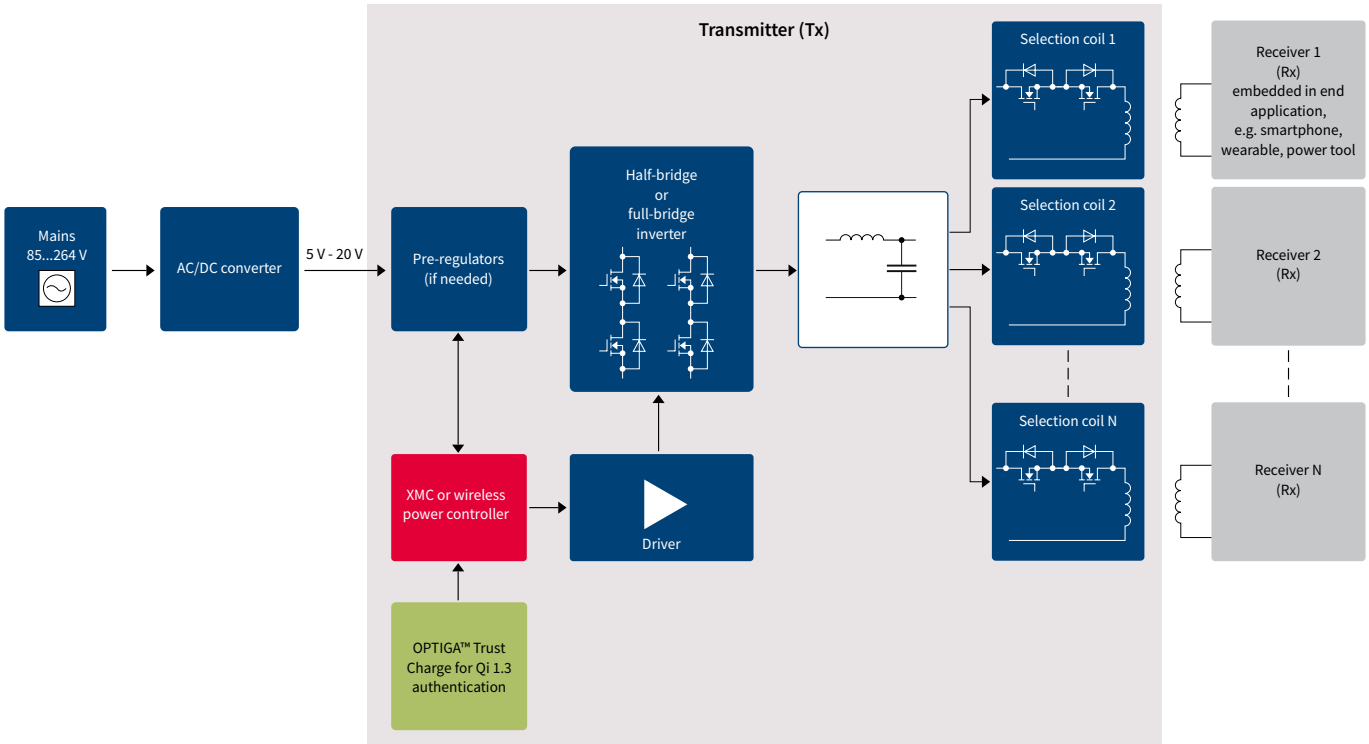

Figure 6: Example wireless transmitter block diagram

In the above example, Infineon's OPTIGA™ Trust Charge provides a separate and secured environment apart from the MCU. This affords isolated and protected storage for the product unit private key and all stored certificates. The OPTIGA™ Trust Charge is built on Common Criteria EAL6+ hardware, meaning that it has built-in countermeasures against common physical attacks as listed previously. Because this security processing is performed on-chip, attackers are hindered from gaining access to secret information by monitoring the main MCU or any onboard communication lines.

The other advantage of this type of architecture is that provisioning can be done with the security IC alone, and not on the assembled device. The OPTIGA™ Trust Charge is provisioned in Infineon's facilities, which have Common Criteria certification and are trusted to produce security ICs in many high-security markets. The OPTIGA™ Trust Charge can be purchased pre-loaded with all of the keys and certificates needed to uniquely identify it as belonging to a specific manufacturer and certified by the WPC (see Figure 7).

It provides a solution that is easy and quick to implement, which doesn't rely on additional process setups or external audits. Additionally, it provides the device manufacturer with revenue and brand protection against counterfeit devices.

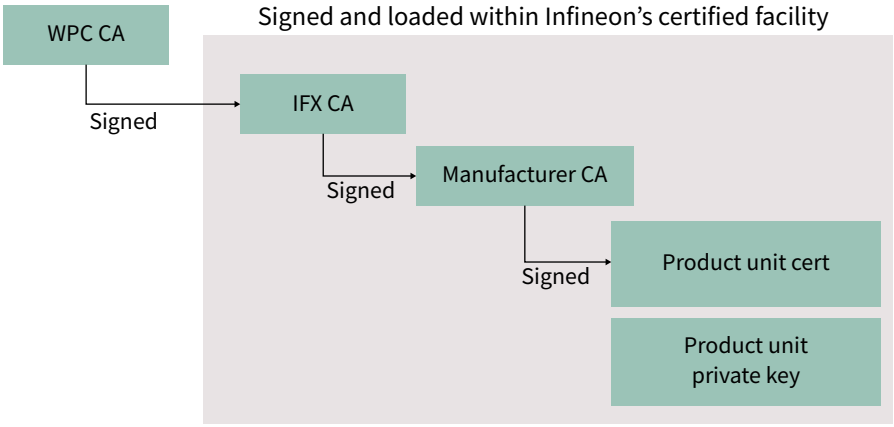

Figure 7: Infineon provisioning setup

Summary

The WPC is doing a lot to promote a healthy ecosystem of wireless charging devices. A major foundation to this effort is checking the safe operation of devices in the market. The authentication requirements detailed in the Qi specification provide assurance that any validated device has been tested and certified for proper connectivity and safety.

The easiest and most cost-effective way to implement the new authentication requirements is using a separate security IC, such as Infineon's OPTIGA™ Trust Charge. This provides a plug-and-play solution that handles the authentication process and comes pre-loaded with all necessary certificates and keys.

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: 10 / 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.