

CRA and RED: Partnering with Distribution

April, 2026

Der Deutsche Innovationspreis
Winner 2025
Large enterprise
Infineon Technologies AG

WINNER
German Sustainability Award 2025

Restricted

Key Takeaways

1. Infineon is leading in security expertise to support customers in their CRA compliance journey, covering broad applications
2. Infineon has been offering and continue to offer webinars, online training courses, technical collaterals on CRA/RED and support security by design
3. Infineon offers broad product portfolio and solutions in compliance with CRA/RED.
   Seek for Infineon's recommendation on selecting the right MCU to comply with CRA/RED
4. Adding a dSE (discrete Secure Element) can simplify manufacturing, improve efficiency, and save costs down the line
5. Contact our official, franchised Distribution Partners to receive the support from the experts certified by Infineon → https://www.infineon.com/contact-us/where-to-buy?ftab=03

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 CRA vs. RED 4

2 CRA Compliance and Why Infineon 8

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 Distribution Certification Program 66

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 **CRA vs. RED** **4**

2 CRA Compliance and Why Infineon 8

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 Distribution Certification Program 66

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

"If everything is connected, everything can be hacked. [...]

This is why we need a European Cyber Defense Policy, including legislation setting common standards under a new **European Cyber Resilience Act**. "

Ursula von der Leyen
President of EU Commission *during 2021 State of the Union address*





The European Commission highlighted the importance of cybersecurity in the **Radio Equipment Directive (RED)** in 2022, and new mandatory cybersecurity requirements for internet-connected radio equipment took effect on August 1, 2025.

Copyright © Infineon Technologies AG 2026. All rights reserved.

How do they compare? RED vs. CRA

RED is fundamentally different from the Cyber Resilience Act (CRA)

RED For safe and reliable radio communication
Applies to all devices using radio frequency communication
Radio performance and cybersecurity requirements
Applies to the final product and not to individual components
Focus: radio performance, EMC, and cybersecurity for radio communication

CRA For comprehensive cybersecurity protection
Applies to all products with digital elements (MCU, MPU, software, IoT)
Comprehensive cybersecurity and data protection
Applies to individual components within a product with digital elements
Focus: complete security across hardware, firmware, software, and entire product lifecycle

On Dec 11, 2027, CRA will take over the RED based on CRA Articles 3. In other words, CRA will be the sole registration on the product cybersecurity, eliminating the need to meet RED specific cybersecurity clauses.

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA imposes chip-level security requirements while RED imposes system-level security requirements

Cyber Resiliency Act

Radio Equipment Directive
EN-18031 Requirements

	PSA L1 / PSA L2	PSA L3 / PSA L4	CC EAL 6+	
Default "Class 0"	**Important products "Class I"**	**Important products "Class II"**	**Critical products**	**All Wireless Products**
Examples: All products with digital elements (HW & SW) not Class I, II or Critical	Examples: Microcontrollers, Microprocessors, and ASICs with security functionalities	Examples: Tamper-resistant Microcontrollers & Microprocessors	Examples: Smartcards or similar devices, including Secure Elements	Examples: Any electrical product which intentionally emits or receives radio waves
	NIST Compliant TRNG			
	Secure Boot			
	Secure Firmware Update & Recovery Capability			
	Processing Isolation			
	Accelerated Cryptography			
	Secure Storage			
		Physical Fault Attack Mitigation – Boot & Run Time		Wireless Comm. Security E.g. WPA3 Enterprise
		Fault Sensor Management System		
		DICE or Hardware Root-of-Trust (RoT)		
			DSI - AVA.VAN.5	

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 CRA vs. RED 4

2 **CRA Compliance and Why Infineon** **8**

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 Distribution Certification Program 66

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

The European Cyber Resilience Act (EU CRA)
Implications for customers

Implications for customers

- **Cybersecurity Requirements**: The EU CRA sets out specific cybersecurity requirements for products with digital elements, including secure-by-design and secure-by-default principles, vulnerability management, and incident response planning that are sold in the EU
- **Full compliance required by December 11th, 2027**
- Linked to established CE Logo
- **Enforced penalties** for unconformity
- **Act now** to ensure compliance by end of 2027

CE

Infineon – a leader in security

- **Security Leader** for more than 25 years, shaping the market
- Deep **system understanding** of embedded applications – **ability to consult** customers directly or through partners
- **Comprehensive product portfolio** tailored to specific needs, from embedded security to stand-alone security products



Copyright © Infineon Technologies AG 2026. All rights reserved.

Short guide to CE labelling process*

**for details visit EU commission website on CE labelling process*

The manufacturer is **responsible for** ensuring **conformity with all relevant EU-wide regulations**, including CRA from 11 Dec. 2027 onwards

For this, the manufacturer would

1. determine whether they can assess the product by themselves or need to involve a notified body
2. put together a technical dossier documenting conformity to EU norms
3. draft and sign an EU declaration of conformity document

Once the product bears the CE marking, if a competent national authority requests, the manufacturer must provide all information and documentation on the product's CE marking

The manufacturer **does not need a license** to put CE label on their products



Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA motivation: Improve cyber resilience in the EU through common cybersecurity standards and well-known CE label

In Scope

- The CRA imposes obligations on **manufactures** and **importers** of digital products **sold in EU single market**.
- Connected HW, SW (incl. remote services) sold within EU
  - **Finished products**



  - **Components**



- Products need to be **designed** and **developed** with security in mind to mitigate **vulnerabilities** and manage **potential risks**.

Incompliance penalties

- Administrative fines **up to 15, 10, or 5 million EUR and/or up to 2.5%, 2% or 1%** of total worldwide annual turnover for preceding financial year (whichever is higher, respectively)
- and **Product recalls** (depending on the risk)

Out of Scope

- Products, which fall under other security EU regulation, e.g.,



Medical Device EU MDR-2	**Automotive** UNECE R155	**Marine Equipment**	**Civil Aviation** certified	**IT, Cloud, SaaS** EU NIS-2

- **Non-commercial projects**, including open-source in so far as an open-source project is not part of a commercial activity.

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA essential requirements for getting the CE label

Product Security Outcomes



Based on **cybersecurity risk** of the product in its operational environment include:

- Security by default
- Unauthorized access protection
- Data confidentiality, integrity
- Security updateability and event logging
- Secured commissioning/ decommissioning

Vulnerability Management Process



- Processes for managing vulnerabilities – **security updates** – min. 5 years
- SBOM management, availability of SW up to 10 years
- **Coordinated Vulnerability Disclosure**: for incidence reporting to EU central point (ENISA) and customers
- Strict reporting timelines of 1-3-14 days

Information & Labelling



- **Central point of contact** for dealing with vulnerabilities
- Duration and type of the support period
- Instructions for security updates, commissioning, decommissioning
- **Intended use of the product** and information on its security properties
- Location of SBOM (if publicly available)

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA Product catogories and conformity assessments

Default "Class 0"	Important products "Class I"	Important products "Class II"	Critical products
'catch-all category' All products with digital elements (HW, SW, including remote data processing) Class I, II, Critical, or exempted	Examples Smart home devices with security functions (locks, camera, alarms etc), routers, modems, connected toys, personal wearables, ID, biometric, access control	Examples Hypervisors and container runtime environments, VPN, Firewalls, Tamper-resistant Microcontrollers, and Microprocessors,	Examples Smartcards and similar devices, smart metering systems, advanced security systems, incl. for crypto-processing,

Conformity Assessment Options

- Internal Control (Module A)
- Internal Control based on EU harmonized standard*

Self-Assessment

- EU Type Examination + Internal Production Control (Module B+C)
- Full Quality Assurance (Module H)
- EU cyber security certification (e.g., EUCC)

External 3rd party Assessment

* EU harmonized standards development are commissioned by EU Commission; in absence, 3rd Party assessment by Notified bodies is required

Copyright © Infineon Technologies AG 2026. All rights reserved.

What is a EU harmonized standard



- Harmonized standards are standards developed on the request of the EU Commission to the recognized EU standardisation organisations
- Their purpose is to be used for assessment of conformity with a EU regulation of products that are placed on the EU market
- They are voluntary. Manufacturers can use other means of conformity assessment of their products with a EU regulation

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA timeline and Infineon Events (not exhaustive)



embedded world Exhibition&Conference

Infineon #1 in MCUs

EE Times

Commission Draft	Council & Parliament Proposals	Final Vote	Entry into Force (adopted)	Implementation Act to CRA*	Entry into Force (adopted)	Incident Reporting Obligations	Product Compliance Obligations
09/22	07/23	03/24	10/24	11 Dec 2025	11 June 2026	11 Sept 2026	11 Dec 2027

+15 months Transition period

Click the event to see more

DISCLAIMER: The timeline is guided by the EU Commission.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Cyber security threats to your application

Type of Risk	Exploitation method	Financial Risk	Impact on CRA compliance
Compromise of Customer Credentials	Cybercriminals can target systems to steal customer login credentials or payment information, leading to identity theft and financial loss.		Yes
Disruption of communication	Large-scale manipulation or attacks on operating systems can overwhelm critical infrastructure and bring down entire networks or systems.		Yes
Data Leakage	Poorly secured backend systems can expose sensitive customer data, including payment information, charging logs, and personal details.		Yes
Ransomware Attacks	Malware can target backend systems, disrupting operations until a ransom is paid.		Yes
SW update attacks	Malware inserted in system during SW/FW updates allowing remote access to manipulate system.		Yes
Unauthorized Operation	Hackers could gain control of chargers, allowing them to disable them, steal electricity, or potentially even disrupt the charging process for other users.		Yes
Unauthorized remote access	Insecure remote connections that allow internet access to control networks, or thru' remote-access accounts with weak passwords.		Yes
…	…		…
…	…		…

Copyright © Infineon Technologies AG 2026. All rights reserved.

Summary of CRA Requirements:

Product Security

- Security by default
- Enable adequate security updates and patches
- Protection from unauthorized access
- Confidentiality and integrity of data, commands and programs
- Minimization of data
- Availability of essential functions
- Minimize own negative impact on other devices
- Limit attack surfaces and reduce impact of an incident
- Record and monitor security relevant events
- Securely, permanently erase and/or transfer data and settings

Documentation

- The following information is requested:
- Manufacturer of the product.
- Central point of contact for dealing with vulnerabilities.
- Instructions for installing security updates.
- Instructions for enabling/disabling automatic security updates.
- Intended use of the product and information on its security properties.
- Known circumstances in its environment that could expose the products to cybersecurity risks.
- Duration and type of the support period.
- Instruction for the secure commissioning, decommissioning and use of the product.
- Location where the SBOM can be accessed (if publicly available).

Vulnerability Report

- Supplier needs processes for managing vulnerabilities and address vulnerabilities without delay
- Supplier needs an organization/platform for the communication of vulnerabilities to
- a) EU central reporting point (ENISA), and
- b) to customers (Coordinated Vulnerability Disclosure).
- If possible, automated security updates and security update information can solve this supporting aspect.
- If technically possible, separate security updates from functional updates.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Cyber Resilience Act (CRA) | Manufacturer responsibilities under the CRA



Security by design

Products must be built with security as a core focus from the start, minimizing cybersecurity vulnerabilities.

Requirement: Conduct a comprehensive risk assessment.



Conformity

Products must meet essential requirements through self-assessment or third-party evaluation.

Requirement: Issue an EU Declaration of conformity and apply the CE marking.



Vulnerability handling

Establish processes and practices to manage vulnerabilities effectively.

Requirement: Report actively exploited vulnerabilities promptly.



Maintenance

Provide support for at least 5 years after the final sale.

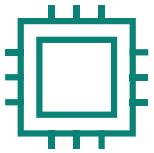
Requirement: Deliver security updates for a minimum of 10 years.

Copyright © Infineon Technologies AG 2026. All rights reserved.

How Infineon can help with CRA compliance



- **Security-by-design:** Infineon security products have this as a core requirement
- **Keys and certificates** provisioned at Infineon's secured, Common Criteria-certified site



- **Security solutions for CRA compliance:** best-fit security solutions to meet CRA security outcomes from a broad range of security products: microcontroller, wireless MCU, discrete secure element, secure memory
- **Software tools:** Infineon's software tools and development platforms facilitate secure development, such as ModusToolbox™, Edge Protect Security Suite
- **Third-party certification:** independent evaluation and certification for standards, such as SESIP, CC, PSA-certified
- **Security lifecycle support for manufacturers:** to address the full product lifecycle, incl. risk assessment, vulnerability management, and reporting.
- **Evaluation platforms:** providing evaluation boards, reference designs, and software/hardware trainings to support design



- **Active in EU CRA standardizations**: contributing and leading EU standardization working groups in CENELEC
- **Decades-long expertise:** knowledge of regulatory requirements and variance of CRA compliance requirements
- **Training support:** Infineon provides resources like webinars to help customers understand and prepare for CRA
- **Implementation collaterals:** security-specific resources, such as, product documentation, security guidance manuals

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon's security solutions mapping to CRA requirements



Required product security capabilities	Security functions offered in Infineon products
Security-by-default Design and Development	Common Criteria, PSA Certified*, SESIP, IoT security standards such as ETSI EN 303 645, IEC 62443 and EN 18031 (ref. Radio Equipment Directive)
Manufactured with security-by-default	20+ years of manufacturing Common Criteria certified products Strong security culture and able to adapt fast to new requirements
Protection against unauthorized access	Authenticated access, physical tamper resistance, secured connection, secured key storage/management, transport protection
Limit attack surfaces	Secured debug interfaces, passive security features (e.g. sensors, memory encryption), security critical information firewalled from processing environment
Adequate security updates	Secure software update, key and credentials management services Business continuity and PSIRT processes for self and customer support

*independent security evaluation scheme for IoT and connected chips, system software and devices with a commitment to update future versions to track important EU CRA regulatory requirements

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon & Cyber Resilience Act – Infineon featured as both Chair & Working Group leader supporting initiative

CENELEC | TC47X | CHAIR (IFX) Uwe Rueddenklau

WG 1	WG 2	WG 3
Processors and Microcontrollers security-related functionalities	Processors and Microcontrollers Tamper-resistant	Smartcards or similar devices, including Secure Elements
CONVENOR (STM) Stephan Courcambeck	CONVENOR (NXP) Eve Atallah	CONVENOR (IFX) Mariela Pavlova

Initial work started – Ad Hoc group initiated

Potential other areas for TC47X standards	WG ASIC-FPGA	WG Security Boxes	WG Smart Metering Gateway

Copyright © Infineon Technologies AG 2026. All rights reserved.

TC47X development of standards for semiconductor platforms



Evaluation Norm	Scope	Level of tamper resistance
EN 50765	MCUs/MPUs with security functionalities optionally with an OS/Application environment	AVA_VAN.1 (basic)
EN 50766	Tamper resistant MCUs/MPUs optionally with an OS/Application environment	AVA_VAN.2-3 (basic – enhanced basic)
EN 50764	Platforms for Smart cards/similar devices/secure elements optionally with an OS/Application environment	AVA_VAN.4-5 (moderate-high)
EN 50767	ASICs and FPGAs with security functionalities	Under development

- The mature drafts of EN 50765, EN 50766 and EN50764 to enter public enquiry phase by end of 2025.
- EN 50767 has been kicked off mid-2025 and in early stage of development.
- AVA_VAN vulnerability assurance levels from the Common Criteria standard require an increasing level of tamper resistance, from basic, enhanced-basic, moderate, to high.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Vulnerabilities reporting and management at Infineon

- By setting rules for identifying, fixing, mitigating, and reporting new vulnerabilities before they are exploited, Coordinated Vulnerability Disclosure (CVD) is crucial for protecting users and strengthening cybersecurity in the EU.
- The vulnerability issues must be reported to the single reporting platform that ENISA has been charged with creating in Article 16 in EU Cyber Resilience Act.
- Infineon's point of contact for reporting: PSIRT@infineon.com

Copyright © Infineon Technologies AG 2026. All rights reserved.

Black Duck: SW for security, quality, SBOM and risk management

- Infineon uses Black Duck to manage the security, quality, and license compliance risks that come from the use of open source and third-party code in applications and containers.
- Key benefits
  - Black Duck's multifactor open source detection technology gives an accurate report of open source present in our applications and container.
  - It does different analyses of the application to ensure accurate result.
  - It integrates with build tools like Maven and Gradle to track both declared and transitive open source dependencies in applications built in languages like Java and C#.
  - It maps strings, files, and directories information to Black Duck KnowledgeBase to identify open source and third-party components in applications built using languages like C & C++.
  - It finds parts of open source code that have been copied within proprietary code, which can potentially expose you to license violations and conflicts. We are using snippet analysis as per our Black Duck OSS Scan
- Blackduck provides the following functions:
  - Scan the code and identify open-source software included in the code base.
  - View the generated Software Bill of Materials (SBOM) for projects.
  - View vulnerabilities identified in open-source components.
  - Assess security, license, and operational risks.



Copyright © Infineon Technologies AG 2026. All rights reserved.

EU CRA challenges faced by manufacturers



- **Understanding** the technical requirements to comply with CRA
- Performing **continuous security assessments** in line with CRA
- Building the **product is built with security in mind from the start**, e.g. secured-by-default configurations that close unnecessary ports, services
- **Establishing Software Bill of Materials** (SBOM) as part of the product's security by design process
- **Tracking, securing 3rd party components** in the supply chain
- **Implementing processes** for continuous monitoring, detection, and assessment of vulnerabilities
- Establishing clear and timely **incident reporting procedures**
- **Delivering ongoing security updates** throughout the product's lifecycle

Copyright © Infineon Technologies AG 2026. All rights reserved.

Your 4-step CRA preparation plan



Understand

- CRA scope, definitions
- Exemptions
- Compliance requirements

Identify

- Affected products
- Components
- Dependencies (build SBOM)

Assess

- Gaps and risk analysis vs CRA Annex I/II
- Plan mitigations

Implement

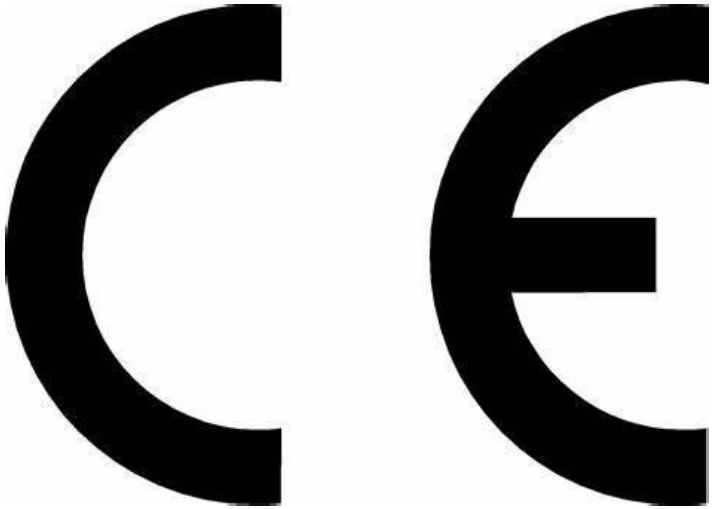
- Security-by-design
- Vulnerability management
- CE documentation, security tests

Copyright © Infineon Technologies AG 2026. All rights reserved.

Evidence and documentation plan – an example

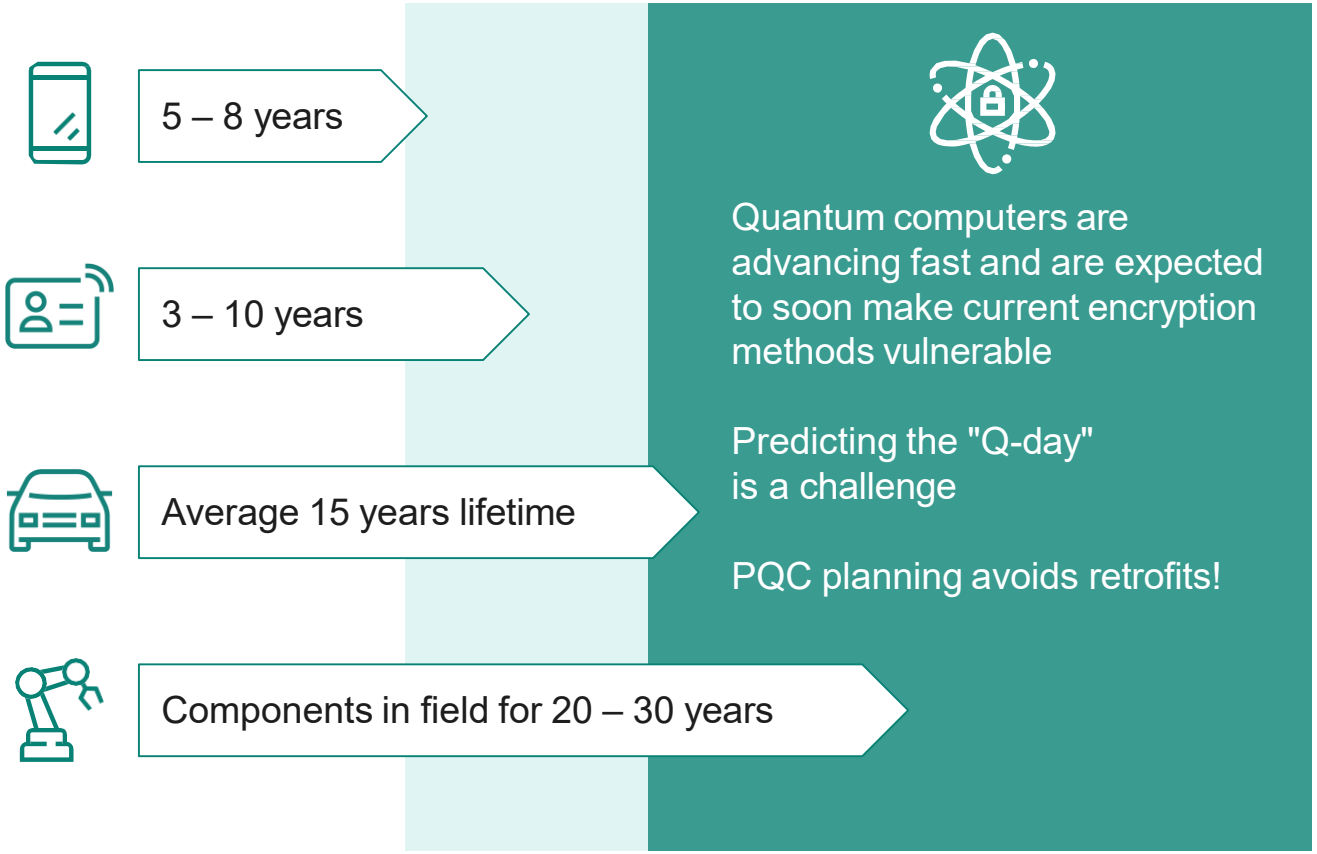
- Risk assessment
- Security evaluation reports
- Release criteria (no known vulnerabilities),
- SBOM including dependencies including 3rd Party components
- User-facing security information and labels
- Vulnerability handling process
- EU declaration of conformity (DoC)

Keep this technical dossier living, that is update on each major release



Copyright © Infineon Technologies AG 202. All rights reserved.

CRA devices with long service life need crypto-agility



Post-Quantum Cryptography
for building cyber resilience post-"Q-day"

- Use crypto-agile algorithms that are not threatened by prime factorization or similar
- Can be implemented on conventional hardware
- Standardized, published, trusted by recognized authority

World's first CC certification for a security controller with a secured PQC implementation
PSOC™ Control C3 Performance Line is the first Infineon MCU with accelerated PQC options

Copyright © Infineon Technologies AG 2026. All rights reserved.

Transition into PQC era – Product Milestone/Timeline

2022

June 2022

First TPM with PQC-protected XMSS FW-update mechanism

2024

December 2024

First CC EAL6 certified crypto library with ML-KEM

August 2025

PSOC™ Control C3 Performance Line First CNSA 2.0 compliant and PSA Certified level 3 MCU family

1st MCU with LMS/XMSS verify Q3/2025

2026

1st MCU with ML-DSA/KEM Q1/2026

Mid 2026

Expected major TCG PQC standards update

All new MCU and comms products with full PQC support Q3/2026

End of 2026

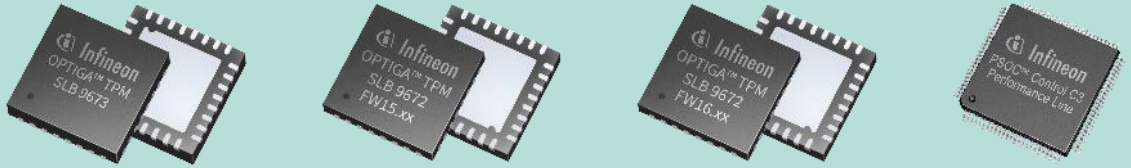
First TPM with PQC-ready HW

2028

End of 2027

First PQC-ready and certified TPM (HW+FW)

Existing and new Hardware



Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 CRA vs. RED 4

2 CRA Compliance and Why Infineon 8

3 **RED Compliance and Why Infineon** **30**

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 Distribution Certification Program 66

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

The more connected our world becomes, the more our devices need to be secured



Why was RED introduced?

With the rising cybersecurity vulnerabilities, the EU has taken the initiative to impose a minimum basic level of security for connected wireless devices

RED aims to ensure that all devices that use radio waves (phones, Wi-Fi routers, Bluetooth speakers) are safe, work properly and don‘t interefere with other devices

What RED mandates

- ✓ Efficient use of radio equipment
- ✓ Prevention of harmful interference
- ✓ Meeting safety and health requirements
- ✓ Meeting cybersecurity requirements (as of August 2025)

RED timeline

RED is adopted by the EU Parliament and Council
05/2014

RED comes into force
06/2014

Cybersecurity requirements added to RED
09/2021

RED cybersecurity requirements finalized
08/2024

Start of first full year RED become mandatory
08/2025



RED essential requirements and harmonized European Norms (hEN)

What to achieve: covered in the RED essential requirements (written as law)	**How to achieve it:** covered in the RED harmonized European Norms Common Security Requirements EN 18031		
(d)* radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service	**Part 1**: Internet-connected radio equipment	Radio equipment with an internet connection, either directly or indirectly.	Smartphones, routers, smart home devices, industrial IoT equipment.
(e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected	**Part 2**: Radio equipment processing personal data	Radio equipment that processes personal data, traffic data, or location data, including internet-connected devices, childcare equipment, toys, and wearables.	Baby monitors, smartwatches, connected toys, wearables.
(f) equipment supports certain features ensuring protection from fraud	**Part 3**: Internet-connected radio equipment processing virtual currencies or monetary values	Internet-connected radio equipment that processes virtual currencies or monetary values.	Mobile payment terminals, digital wallets, connected POS systems.

*(d), (e), (f): New essential requirements added to RED to foster cybersecurity

Copyright © Infineon Technologies AG 2026. All rights reserved.

Component compliance and choosing the right partner is still crucial for RED compliance



RED compliance applies to the entire final product

While individual components alone do not guarantee compliance, **choosing the right components - and the right partner** - can significantly support and accelerate the path to RED conformity.

A chip might meet all technical requirements and standards if

- Used correctly
- Is combined with secured software
- Is placed in a device designed with security in mind

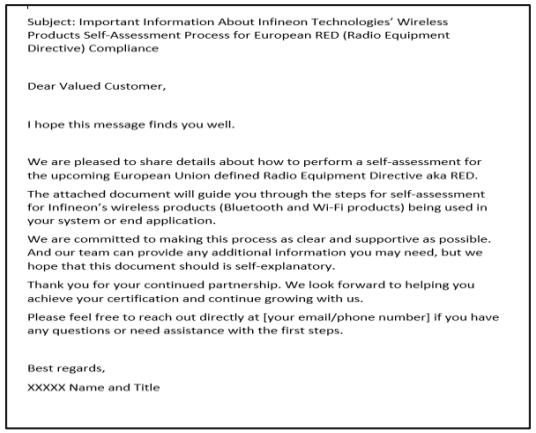
Why Infineon is the right partner to help you achieve RED compliance

- Our solutions consist of hardware, software and servies - this enables us to step in and **support manufacturers with a majority of the tasks** associated with obtaining RED compliance
- We bring decades-long expertise and **in-depth knowledge of regulatory requirements** to all critical components and stages of RED compliance

EU RED Compliance Model For Infineon Products – Infineon can provide Self-Attestation Letter & Table, 3rd Party Attestation with Accredited Lab

- **Who needs to be compliant to RED?**
  - Device manufacturers i.e. anyone who sells consumer products that have a wireless transmitter. Examples of such products are smart phones, wearables, cameras, laptops etc.
- **What do device manufacturers have to do?**
  - They need to either perform a self-assessment as per CENELEC EN 18031, or
  - They need to contract and use a RED Notified body
  - Finally, they need to fill-in and sign the EU declaration of conformity, and store this for 10 years for access at any time.
- **Infineon can help device manufacturers who purchase our wireless SoCs in the following manner:**
  - **Connected MCU Products** : Provide Infineon's attestation of conformity to 18031 for Connected MCU products that can be re-used for final RED compliance assessment.
  - **Wi-Fi/BT Combo Products** : These products can be used in a secured system in support of the EU Radio Equipment directive by pairing with an adequately secured MPU/MCU.

Self-Attestation Letter



Subject: Important Information About Infineon Technologies' Wireless Products Self-Assessment Process for European RED (Radio Equipment Directive) Compliance

Dear Valued Customer,

I hope this message finds you well.

We are pleased to share details about how to perform a self-assessment for the upcoming European Union defined Radio Equipment Directive aka RED.

The attached document will guide you through the steps for self-assessment for Infineon's wireless products (Bluetooth and Wi-Fi products) being used in your system or end application.

We are committed to making this process as clear and supportive as possible. And our team can provide any additional information you may need, but we hope that this document should is self-explanatory.

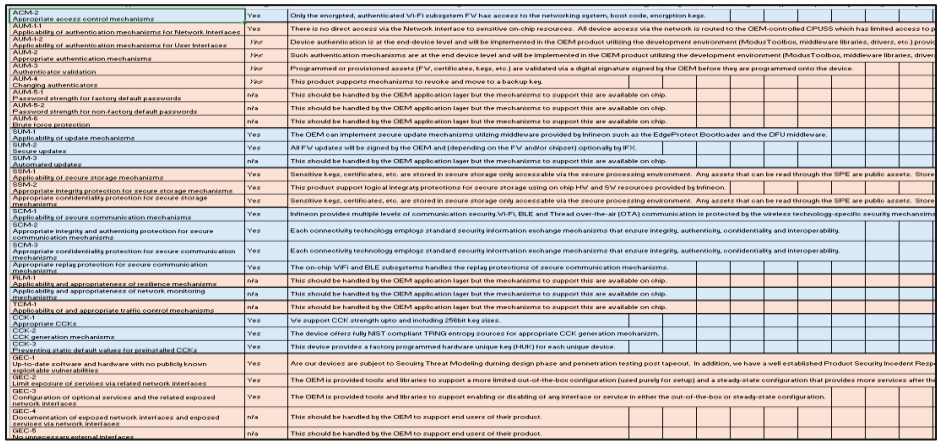
Thank you for your continued partnership. We look forward to helping you achieve your certification and continue growing with us.

Please feel free to reach out directly at [your email/phone number] if you have any questions or need assistance with the first steps.

Best regards,

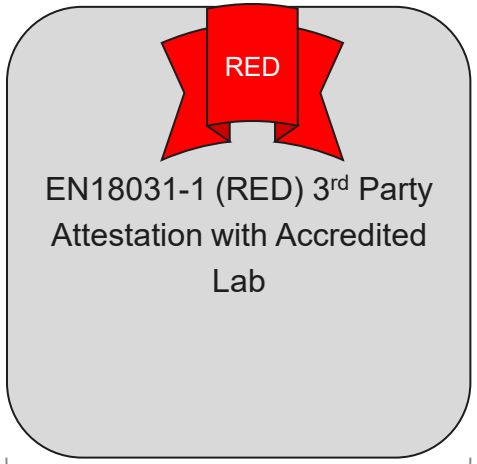
XXXXX Name and Title

Self-Attestation Table



ACM-2 Appropriate access control mechanisms	Yes	Only the encrypted, authenticated Wi-Fi subsystem FW has access to the networking system, boot code, encryption keys.
AUM-1 Applicability of authentication mechanisms for Network Interfaces	Yes	There is no direct access via the Network interface to sensitive on-chip resources. All device access via the network is routed to the OEM-controlled CPUSS which has limited access to p
AUM-1.2 Applicability of authentication mechanisms for User Interfaces	Yes	Device authentication is at the end-device level and will be implemented in the OEM product utilizing the development environment (ModusToolbox, middleware libraries, drivers, etc.) provic
AUM-2 Appropriate authentication mechanisms	Yes	Such authentication mechanisms are at the end device level and will be implemented in the OEM product utilizing the development environment (ModusToolbox, middleware libraries, driver
AUM-3 Authenticator validation	Yes	Programmed or provisioned assets (FW, certificates, keys, etc.) are validated via a digital signature signed by the OEM before they are programmed onto the device.
AUM-4 Changing authenticators	Yes	This product supports mechanisms to revoke and move to a backup key.
AUM-5.1 Password strength for factory default passwords	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
AUM-5.2 Password strength for non-factory default passwords	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
AUM-6 Brute force protection	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
SUM-1 Applicability of update mechanisms	Yes	The OEM can implement secure update mechanisms utilizing middleware provided by Infineon such as the EdgeProtect Bootloader and the DFU middleware.
SUM-2 Secure updates	Yes	All FW updates will be signed by the OEM and (depending on the FW and/or chipset) optionally by IFX.
SUM-3 Automated updates	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
SSM-1 Applicability of secure storage mechanisms	Yes	Sensitive keys, certificates, etc. are stored in secure storage only accessable via the secure processing environment. Any assets that can be read through the SPE are public assets. Store
SSM-2 Appropriate integrity protection for secure storage mechanisms	Yes	This product support logical integrity protections for secure storage using on chip HW and SW resources provided by Infineon.
SSM-3 Appropriate confidentiality protection for secure storage mechanisms	Yes	Sensitive keys, certificates, etc. are stored in secure storage only accessable via the secure processing environment. Any assets that can be read through the SPE are public assets. Store
SCM-1 Applicability of secure communication mechanisms	Yes	Infineon provides multiple levels of communication security.Wi-Fi, BLE and Thread over-the-air (OTA) communication is protected by the wireless technology-specific security mechanisms
SCM-2 Appropriate integrity and authenticity protection for secure communication mechanisms	Yes	Each connectivity technology employs standard security information exchange mechanisms that ensure integrity, authenticity, confidentiality and interoperability.
SCM-3 Appropriate confidentiality protection for secure communication mechanisms	Yes	Each connectivity technology employs standard security information exchange mechanisms that ensure integrity, authenticity, confidentiality and interoperability.
SCM-4 Appropriate replay protection for secure communication mechanisms	Yes	The on-chip WiFi and BLE subsystems handles the replay protections of secure communication mechanisms.
RLM-1 Applicability and appropriateness of resilience mechanisms	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
MCM-1 Applicability and appropriateness of network monitoring mechanisms	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
TCM-1 Applicability of and appropriate traffic control mechanisms	n/a	This should be handled by the OEM application layer but the mechanisms to support this are available on chip.
CCK-1 Appropriate CCKs	Yes	We support CCK strength upto and including 256bit key sizes.
CCK-2 CCK generation mechanisms	Yes	The device offers fully NIST compliant TRNG entropy sources for appropriate CCK generation mechanism.
CCK-3 Preventing static default values for preinstalled CCKs	Yes	This device provides a factory programmed hardware unique key (HUK) for each unique device.
GEC-1 Up-to-date software and hardware with no publicly known exploitable vulnerabilities	Yes	Are our devices are subject to Security Threat Modelling during design phase and penetration testing post tapeout. In addition, we have a well established Product Security Incedent Resp
GEC-2 Limit exposure of services via related network interfaces	Yes	The OEM is provided tools and libraries to support a more limited out-of-the-box configuration (used purely for setup) and a steady-state configuration that provides more services after the
GEC-3 Configuration of optional services and the related exposed network interfaces	Yes	The OEM is provided tools and libraries to support enabling or disabling of any interface or service in either the out-of-the-box or steady-state configuration.
GEC-4 Documentation of exposed network interfaces and exposed services via network interfaces	n/a	This should be handled by the OEM to support end users of their product.
GEC-5 No unnecessary external interfaces	n/a	This should be handled by the OEM to support end users of their product.

3rd Party Assessment



For Connected MCUs and Combo Companions

For Connected MCUs

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1	CRA vs. RED	4
2	CRA Compliance and Why Infineon	8
3	RED Compliance and Why Infineon	30
4	**Infineon's Response to CRA/RED**	**36**
5	Infineon Solution Compliant with CRA/RED	40
6	Security Related Collaterals	60
7	Distribution Certification Program	66
8	Key Takeaways	68

Copyright © Infineon Technologies AG 2026. All rights reserved.

What industry is saying about Infineon’s significant actions on CRA/RED for customers

- **Security Solutions Portfolio:** Infineon offers a wide range of hardware and software security products to meet CRA and RED requirements, including **SECORA™**, **OPTIGA™**, **PSoC™**, **AIROC™ Wi-Fi and Bluetooth**, and **SEMPER™ Secure**.
- **"Secure by Design" Support:** Infineon is focusing on helping manufacturers integrate security from the start, covering aspects like secure boot, cryptographic authentication, and secure firmware updates to protect against IoT threats.
- **Expert Consulting:** Infineon provides security experts to assist customers in navigating the complex legal and technical requirements of the CRA and RED.
- **Educational Initiatives:** In collaboration with distribution partners, Infineon is holding webinars to educate the industry on CRA compliance, including vulnerability management and documentation.
- **Supply Chain Security:** Beyond the product, Infineon is working on strengthening the entire ecosystem's resilience to comply with the legislation's emphasis on product lifecycle security.
- **Pre-Certified Modules:** To help customers skip extensive testing (such as EN 300 328), Infineon provides modules that are already RED compliant, reducing the time and cost for end-product certification.
- **Security Documentation and Lifecycle Management:** Assisting manufacturers in preparing necessary documentation, such as the Software Bill of Materials (SBOM), and managing security updates for the required minimum of 5 years.
- **Vulnerability Disclosure Support:** Establishing policies that allow customers to receive information about known issues and report vulnerabilities, in line with the CRA's reporting obligations.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Web Resources on CRA/RED

Web Resources	Key Messages
CRA landing page	Infineon's CRA landing page, including information on what CRA is, list of core requirements for compliance, benefits of CRA, how Infineon supports IoT customers to achieve CRA compliance, and Infineon's CRA starter guide, etc.
RED landing page	Infineon's RED landing page, highlighting what RED delegated article applies, how to become RED compliant, and how Infineon can help.
Interview on CRA with Thomas Rosteck	"The Electronics Maker" magazine interviewed Thomas Rosteck, President of Connected Secure Systems (CSS) division at Infineon, discussing the CRA's objectives, its impact on global and Indian manufacturers, and how companies can stay ahead of evolving cybersecurity regulations.
EETimes podcast	In this podcast, Preeti Ohri Khemani, our Sr. Director for IOT's Ecosystem Development, talks about the implications of the CRA, not just for Europe but for the global supply chain, and the timeline and some of the things embedded systems developers need to be addressing now.
Infineon CRA blog	This blog on our community site talks about why CRA, what is in and out of the scope, the essential requirements, timeline CRA becomes in effect, and more importantly what Infineon can help.
EU Legislation on CRA	EU's regulation 2024/2847 on horizontal cybersecurity requirements for products with digital elements (CRA)
Infineon ranked #1 in MCUs	Infineon takes over the number one position in the global microcontroller market. According to the latest research by Omdia, the company increased its market share to 21.3 percent in 2024 (2023: 17.8 percent), achieving the largest year-over-year gain (3.5 percentage points) among its competitors. This makes Infineon the most successful supplier of microcontrollers worldwide for the first time in the company's history.

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA/RED Go-To-Market Collaterals

Collaterals and Links	Target Audience	Type of Collateral	Date Updated	Version
MAPS2	S/M/AE/FAE/D/R		TBA	
Customer presentation: CRA/RED	Customers		TBA	
Get Ready for EU Cyber Resilience Act with Infineon	Public	Video/PDF	Nov 5, 2025	
Navigating the EU CRA with Infineon	Public	Video/PDF	Mar 4, 2025	
Cyber Security Aspects of the European RED	S/M/AE/FAE/D/R	Video/PDF	Aug 8, 2024	Ver 1.0
Introducing the EU CRA: C-level and management	Customer C-level	Video	Jun 27, 2025	Ver 2.0
Introducing the EU CRA: Department heads and decision makers	Customer management	Video	Aug 8, 2025	Ver 1.0
CRA: customer and background info	Customers	PPT	Jun 25, 2025	
Strengthening Cybersecurity in the EU: Navigating the CRA	D/R	Video	Sept 16, 2025	
The global security regulations landscape with focus on CRA	Customers	Video	Dec 18, 2024	Ver 3.0

S: Sales M: Marketing AE: Application Engineer FAE: Field Application Engineer D: Distributor R: Rep

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1	CRA vs. RED	4
2	CRA Compliance and Why Infineon	8
3	RED Compliance and Why Infineon	30
4	Infineon's Response to CRA/RED	36
5	**Infineon Solution Compliant with CRA/RED**	**40**
6	Security Related Collaterals	60
7	Distribution Certification Program	66
8	Key Takeaways	68

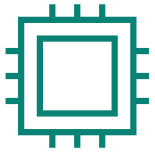
Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon acceletrates CRA compliance for your products



Security-by-design

Secured key/certificate provisioning and PQC-ready controllers/MCUs to speed conformity evidence



Solutions and Tools

Certified components, software tools and reference platforms with lifecycle support with SBOMs and security updates



Expertise and Enablement

EU standards leadership, decades of security product and process experience, training and implementation collateral

Copyright © Infineon Technologies AG 2026. All rights reserved.

The CRA checklist: 5 mandatory security outcomes...

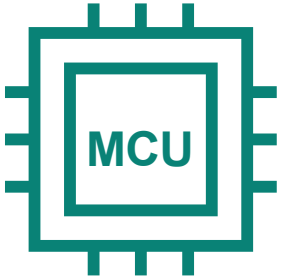
...and how Infineon products help fulfil them

CRA obligation	Engineering requirement	Infineon solution/s
Secure-by-design	Protected Root of Trust	PSOC™ Edge 8x, PSOC Control C3 OPTIGA™ TPM, OPTIGA™ Trust M
Security Updates	Authenticated OTA Update	PSOC™ MCUs: Edge 8x, Conrol C3 OPTIGA™ TPM, OPTIGA™ Trust M
Data Protection	Isolated Key Storage	OPTIGA™ TPM, OPTIGA™ Trust M PSOC™ MCUs: Edge 8x, Conrol C3
Incident Logging	Security Audit Logs & Attestation	OPTIGA™ TPM
Vulnerability Management	Secured Lifecycle Management/ Provisioning/PSIRT	PSOC™ MCUs: Edge 8x, Conrol C3 OPTIGA™ TPM, OPTIGA™ Trust M

Copyright © Infineon Technologies AG 2026. All rights reserved.

Almost every connected device needs a

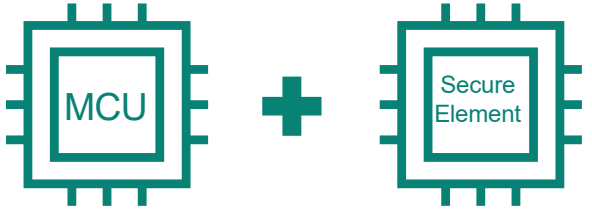
MCU/ MPU



?

When does it need a dedicated

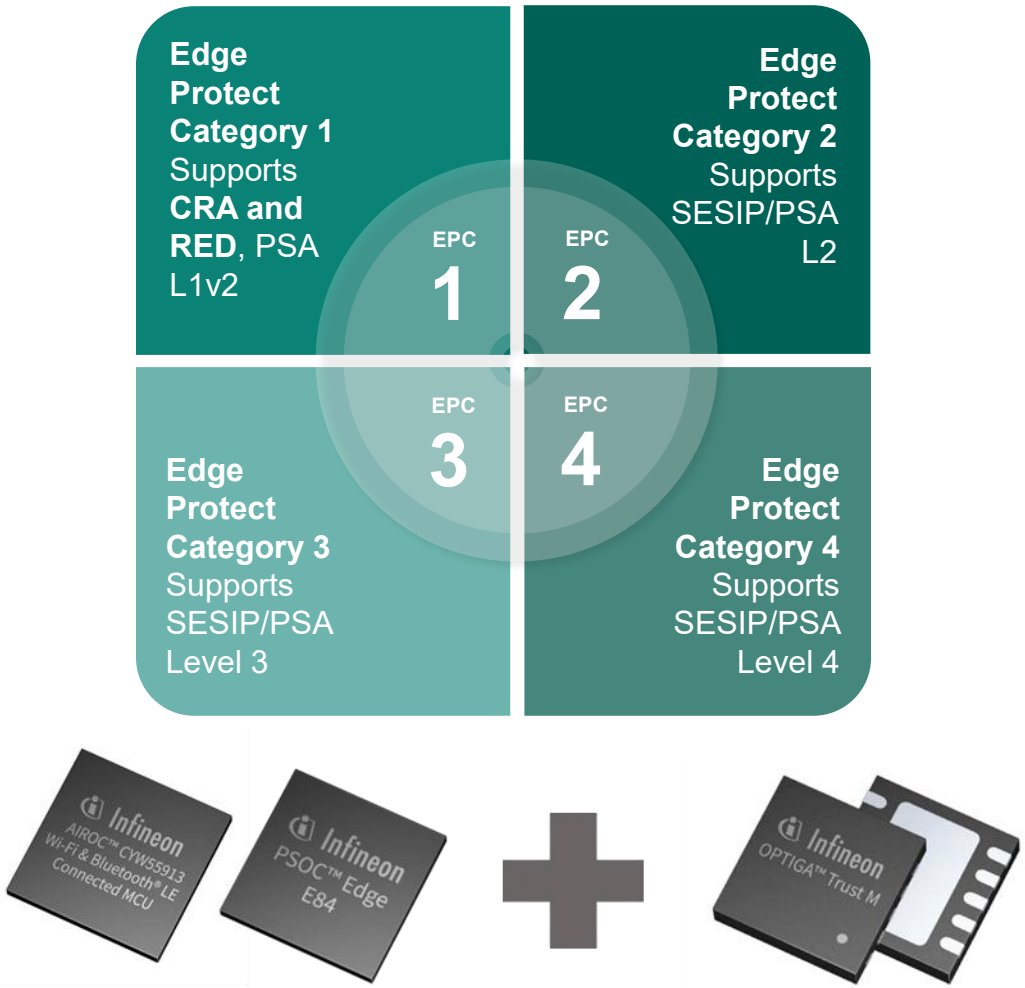
HW-security-anchor?



Edge Protect family integrates leading security-hardened MCU and Discrete Secure Elements so sales and customers can easily find the right fit for their products and applications.

- Choose the best fitting **PSOC™** microcontrollers
- Know when to extend your system with a discrete Secure Element (dSE)
  - Our discrete Secure Elements from **OPTIGA™** work in tandem with each PSOC.
  - Adding a dSE can simplify manufacturing, improve efficiency, and save costs down the line.

MCU with or without Secure Element: We make the choice easy



Copyright © Infineon Technologies AG 2026. All rights reserved.

The right combination of MCU and dSE enables system design with the right modularity and efficiency

Security features	EPC 1 MCU Minimum MCU Requirements CRA/RED PSA L1v2	+ dSE	EPC 2 MCU Additional wireless connectivity security services | SESIP/PSA L2	+ dSE	EPC 3 MCU Hardened Crypto and Fault, Glitch mitigation SESIP/PSA L3	+ dSE	EPC 4 MCU Hardware isolated, lockstep Secure Enclave (SE) | SESIP/PSA L3+SE	+ dSE
Cryptography	✓	+	✓	+	✓	+	✓	+
Secure Boot	✓		✓		✓		✓	
Secure FW Update	✓		✓		✓		✓	
Processing isolation	✓		✓		✓		✓	
Compliance with CRA/RED	✓		✓		✓		✓	
Prebuilt security stack with secured key storage		+	✓	+	✓	+	✓	+
Physical glitch hardening					✓		✓	
Security fault management system					✓		✓	
Hardware isolated Secure Enclave		+		+		+	✓	+
Pre-configured credentials		+		+		+	✓	+
Value-adds (FIPS, TPM, NFC, Payment, …)		+		+		+	✓	+
Late-stage provisioning, machine ID, and key injection in secured environment		+		+		+		+
High-security anti-cloning and device identity protection		+		+		+		+

dSE = discrete Secure Element

Copyright © Infineon Technologies AG 2026. All rights reserved.

How do Infineon's embedded products map to the CRA categories*

Product mapping				
CRA categories	**Default** "Unclassified"	**Important** "Class I"	**Important** "Class II"	**Critical** **Products**
Class Specification	**Approximately 90% of products fall into this category**, which has a lower risk profile compared to other categories.	These are the products that present a higher cybersecurity risk (in terms of its intensity and ability to damage the health, security, or safety of users of such products) and should undergo a stricter conformity assessment procedure. **Class II** products hold a **higher level of criticality** and are thus subject to more stringent compliance measures, including **assessment by external third parties.**		These products have **cybersecurity-related functionality** that poses **a significant risk of adverse effects**, potentially disrupting or damaging multiple digital products.
Conformance	**Self assessment** Manufacturers can use Module A (internal control) to certify compliance rather than needing a third-party auditor	**Harmonized Standard (hEN)**** Manufacturers shall use hEN if self-assessment or 3rd party assessment to demonstrate that products comply with an EU legislation (e.g. EN 50765).	**Harmonized Standard (hEN)** and 3rd party assessment** Manufacturers shall use 3rd party assessment to demonstrate that products comply with an EU legislation	**EUCC** – European Cybersecurity Certification** A scheme ENISA is developing on behalf of the European Commission to create a framework to certify products with digital elements meet the essential requirements of the CRA. **EN50764**[1] – standard for smart cards and eSE platforms.
Infineon products enabling CRA	**MCU** – PSOC™3 – PSOC™4 / BLE – PSOC™5 **Wi-Fi** – CYW43022 – CYW43012 – CYW4373E – CYW5459x – CYW43907/53907 **BTBLE** – 2070x/89072 – 20719/20721 – 20819/20820/89820 – 20736/20737 – 20835 – 30739	**MCU** – PSOC™ 61/62/63 with BLE 20829 – WiFi6 IoT Combo – PSOC™ Edge8x – PSOC™ with BLE – PSOC™ Control C3 – WiFi6 Auto Combo **Wi-Fi** – AIROC™ CYW5551x – AIROC™ CYW5557x **Wi-Fi MCU** – AIROC™ CYW5591x – PSW31xx WiFi/BT MCU – PSB3xxx BT MCU **Secure Memory** – SEMPER™ Secure	**MCU (Tamper-resistant MCUs)** – PSOC™ Edge8x **Security controllers** – OPTIGA™ Trust M std. – OPTIGA™ Trust MTR – OPTIGA™ Trust M – Express – OPTIGA™ Authenticate	**Secure Elements (eSE)**[2] – OPTIGA™ TPM (Common Criteria certified) – OPTIGA™ Connect – SECORA™

***Please note that the table is indicative and based on preliminary guidance;** it is subject to changes based on development of CRA harmonized standards, CRA implementation Acts, and any EU Commission- or ENISA- issued CRA guidance.
**Kindly note that the information provided here is intended for informational purposes only and does not constitute legal advice. The official text of the CRA supersedes the explanations provided here.
1 Until the EU Commission issues Delegated Acts allowing or requiring EUCC certification, Critical products must follow Class II assessment (Module B+C or H) and apply standards such as EN 50764
2 CRA requirements can be fulfilled with many MCUs and a discrete Secure Element can make the process easier and more efficient.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Mapping of applications to CRA categories*

Application/Example mapping				
CRA categories	**Default** "Unclassified"	**Important** "Class I„[1]	**Important** "Class II"	**Critical** **Products**
Conformance	**Self assessment** Manufacturers can use Module A (internal control) to certify compliance rather than needing a third-party auditor.	**Harmonized Standard (hEN)**** Manufacturers shall use hEN if self-assessment or 3rd party assessment to demonstrate that products comply with an EU legislation (e.g. EN 50765).	**Harmonized Standard (hEN)** and 3rd party assessment** Manufacturers shall use 3rd party assessment to demonstrate that products comply with an EU legislation	**EUCC** – European Cybersecurity Certification** A scheme ENISA is developing on behalf of the European Commission to create a framework to certify products with digital elements meet the essential requirements of the CRA. **EN50764**[2] – standard for smart cards and eSE platforms.
Examples of Applications and Solutions w.r.t. CRA categories[1]	**Applications where the function is mechanical, electrical, or non-security digital control.** **Consumer Electronics** Adapters & chargers, Audio systems, speakers, soundbars, Smart TVs (non-security parts) **Home Appliances** Air purifiers, Ceiling fans, Coffee machines, Basic vacuum cleaners, Hair dryers & stylers, Induction cooking, Smart Refrigerators/ freezers, Smart Washing/drying	**Connected devices with cybersecurity relevance but not tamper-resistant** **Consumer Electronics** Smart speakers, Smart conference systems, Drones with wireless connectivity **Healthcare & Lifestyle** Connected health wearables (fitness trackers, smart watches), Connected medical monitoring devices (IoT health sensors) **Home Appliances** Products that protect physical security of customers in a residential setting and which can be controlled remotely e.g. Smart door lock, baby monitors, alarm systems etc. **Operating Systems and Security Software** Core Systems: Desktop/mobile operating systems, web browsers, boot managers, and password managers **Identity and Access Management (IAM)** Access Control and Ticketing, authentication readers (including biometrics), and PKI/digital certificate software	**Examples of Class II applications include Hypervisors and container runtime systems; Firewalls, intrusion detection and prevention systems**	**Secure elements, smartcards, eID, payment-grade security hardware** **Hardware Devices with Security Boxes:** Specialized hardware designed to protect and transfer data securely. **Smart Meter Gateways:** Devices used within smart metering systems (as defined in Directive (EU) 2019/944). **Smartcards or Similar Devices:** Devices incorporating a secure element, such as hardware security modules (HSMs) or secure crypto-processing devices. **Advanced Security Components:** Other devices for advanced security purposes, including secure crypto processing.

***Please note that the table is indicative and based on preliminary guidance;** it is subject to changes based on development of CRA harmonized standards, CRA implementation Acts, and any EU Commission- or ENISA- issued CRA guidance.
**Kindly note that the information provided here is intended for informational purposes only and does not constitute legal advice. The official text of the CRA supersedes the explanations provided here.
1 The complete list of products that fall into Important Class I can be found in Annex III of the CRA.
2 Until the EU Commission issues Delegated Acts allowing or requiring EUCC certification, Critical products must follow Class II assessment (Module B+C or H) and apply standards such as EN 50764

Copyright © Infineon Technologies AG 2026. All rights reserved.

Choosing the right security controller for your CRA device

PSOC™ Edge 8x "secured compute for Edge-AI"

- Secured boot with protected root of trust and cryptographic verification.
- Hardware cryptography accelerators (e.g., AES, SHA, ECC) and TRNG.
- Secured lifecycle states and controlled debug; anti-rollback counters.
- Trusted execution capabilities (e.g., memory protection, privilege separation).
- OTA update enablement with authentication and integrity checks.

OPTIGA™ TPM "platform integrity & attestation"

- Ease of provisioning and lifecycle management with SE
- Secured by design/default with TCG 2.0-compliant TPM; measured boot with PCRs; remote attestation.
- Strong key storage and crypto operations offload.
- Device identity anchored in hardware root-of-trust. Support for secured communication (TLS).
- Anchor SBOM integrity via sealed hash.

OPTIGA™ Trust M "IoT security made easy"

- Secure Element (SE) with ECC, symmetric crypto, secured key storage.
- Trust M Express: pre-provisioned certificates to accelerate cloud onboarding and manufacturing.
- Offload TLS mutual authentication; protects credentials from firmware exposure.
- Confidentiality and integrity for keys/operations- supports lightweight integrity checks.

... to enable EU CRA Security outcomes

- Security by design/default, secured update, integrity protection, documentation-friendly features.
- Integrity and authenticity of platform state; secured credentials; supports logging and incident response posture.
- Strong device identity, secured communication, simplified provisioning and update pathways.

Copyright © Infineon Technologies AG 2026. All rights reserved.

PSOC™ Secured MCUs

PSOC™ EDGE



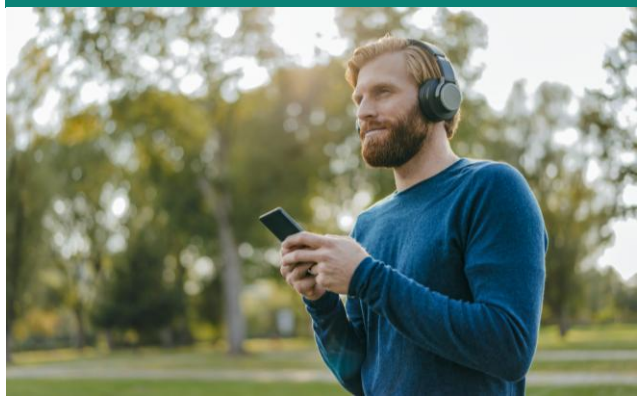
Best-in-class MCU for Edge AI applications allowing customers to create differentiated products for the IoT era while protecting their IPs (models) with the highest security level. Staged AI pipeline enables unrivaled performance to power ratio.

PSOC™ CONTROL



Industrial MCU family maximizing software re-use and scalability to reduce development cost and time-to-market. Rich feature set paired to high performance core allows for maximum efficiency in motor control and power conversion applications.

PSOC™ Connect™



Combining the most advanced MCU and wireless capabilities into a single package and leveraging the most advance security features and architecture on the market.

PSOC™ 6 Family



Proven balance between performance and low power, with security features and capabilities that enable OEMs to configure security for a myriad of use cases.

Copyright © Infineon Technologies AG 2026. All rights reserved.

AIROC™ Secured WiFi and Bluetooth SOCs

AIROC™ WiFi



- AIROC™ Wi-Fi combo products integrate Wi-Fi and Bluetooth in a single-chip to enable small-form-factor IoT designs
- Best-in-class Wi-Fi/Bluetooth range performance and ultra low power consumption enable wide range of applications in smart home, industrial, and automotive

AIROC ™ WiFi MCU



- Highly integrated Wi-Fi/Bluetooth MCU with on-chip microcontrollers, memory, networking stack, and peripherals required for customers to easily create cloud-connected solutions.
- Best-in-class Wi-Fi/Bluetooth range performance and ultra low power consumption enable wide range of IoT applications

AIROC™ Bluetooth



- The most deployed & Interop tested Bluetooth Controller and Host Stack in the industry.
- The modular architecture makes it ideal for Combo devices as well as discrete Bluetooth LE MCUs

AIROC™ Bluetooth MCU

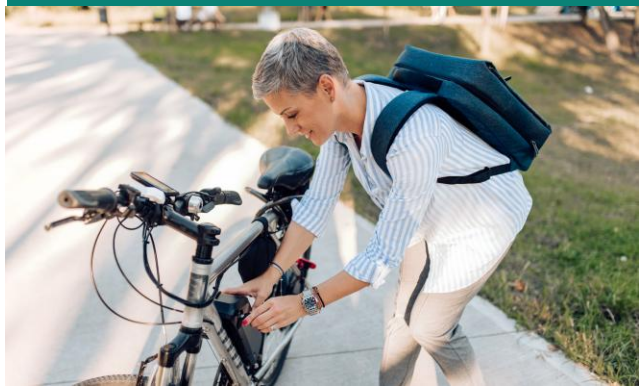


- Highly integrated MCU with Analog and Digital peripherals, high speed ARM Core coupled with a dedicated Bluetooth subsystem
- AIROC™ Bluetooth MCUs are used across various applications where Compute along with connectivity are required

Copyright © Infineon Technologies AG 2026. All rights reserved.

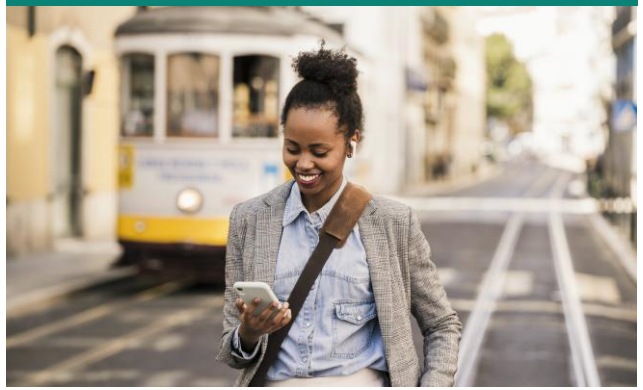
OPTIGA™ embedded security solutions

OPTIGA™ Authenticate



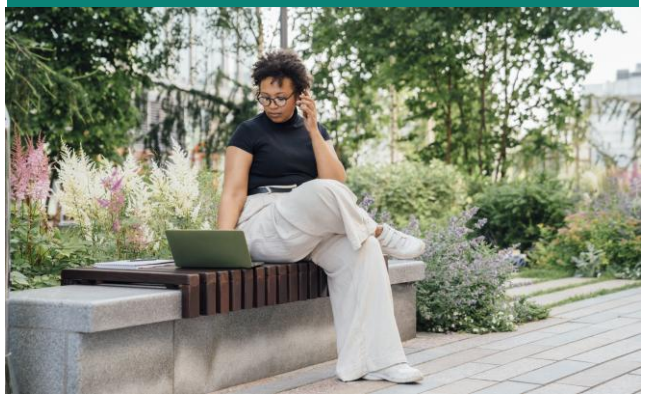
Strong turnkey solutions combining robust hardware security and genuine user experience to verify authenticity of devices and systems to support brand protection and anti-counterfeit measures

OPTIGA™ Connect



Turnkey eSIM security solutions for easy, flexible and secured cellular IoT connectivity at scale for M2M & consumer device applications

OPTIGA™ TPM



Security controllers based on TCG (Trusted Computing Group) specifications protecting integrity and authenticity of embedded devices and systems

OPTIGA™ Trust



Secure Element (SE) offering Common Criteria EAL6+ certified tamper-resistant protection for smart homes, smart building and industrial automation.

Copyright © Infineon Technologies AG 2026. All rights reserved.

SECORA™ family of security solutions

SECORA™ Blockchain



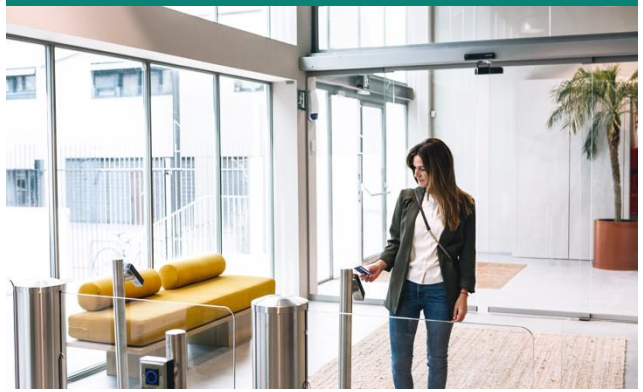
Fast, easy-to-use Java Card™ solution supporting best-in-class security for blockchain system implementation.

SECORA™ Connect



System solution for smart wearable to provide contactless secured payment, ticketing or access applications via Near Field Communication (NFC).

SECORA™ ID



Ready-to-go Java Card™ solution optimized for all electronic identification (eID) applications allowing maximized customization for local needs.

SECORA™ Pay



A complete portfolio for everything from contact cards to smart payment accessories, combined with the latest EMV-ready applications, to meet regional market requirements.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Introducing SEMPER™ Secure Memory

ROBUST SECURITY

World's most-secure NOR Flash Memory

- Hardware root-of-trust
- End-to-end protection
- Flexible architecture

LOW TOTAL COST OF OWNERSHIP

First NOR Flash to combine safety with security

- Advanced functional safety and reliability
- ISO 26262 ASIL-B compliance; ASIL-D ready
- Real-time safety diagnostics and reporting

FAST TIME TO MARKET

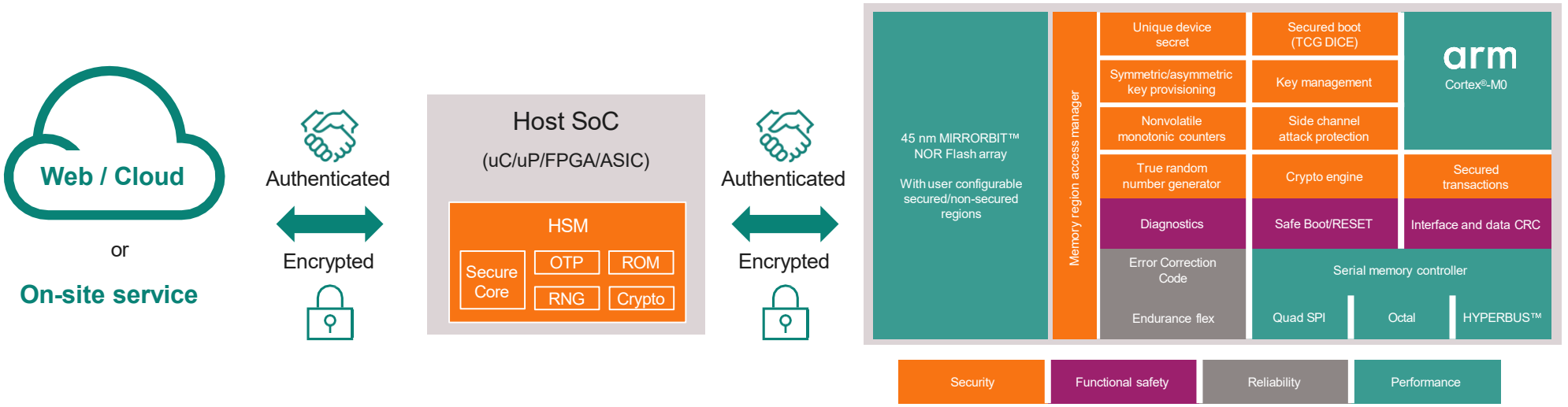
Easy-to-use

- Software Development Kit (SDK) to accelerate development
- Standards-based: TCG DICE-based; NIST CAVP and NIST ESV (Entropy Source Validation)
- Broad chipset and solution partner ecosystem
- PSA Level 1 Certified



Copyright © Infineon Technologies AG 2026. All rights reserved.

Semper Secure Memory: adding security to NOR Flash Memory systems with minimal cost or for flashless-based microcontrollers



Density
Lead: 256 Mb
Concept: 128 Mb, 512 Mb, 1 Gb

Voltage
1.8 V and 3.0 V

Performance
JEDEC xSPI: 400 MB/s
QSPI: 102 MB/s

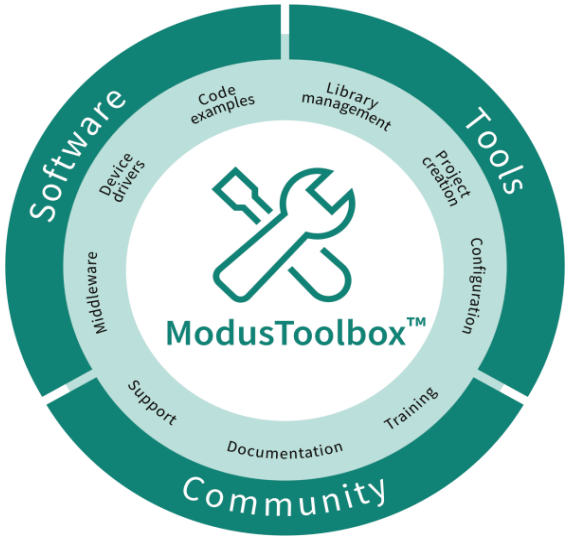
Reliability
500K+ cycles endurance
25 years retention

Package & Temp
BGA, SOIC, WSON
-40°C to 125°C
AEC-Q100 available

Secure Boot	Verify stored boot code integrity without additional overhead. Secure root-of-trust boot
Secured Storage	User-defined regions with selectable security access levels Secured authenticated transactions with a paired SoC (no unauthorized source)
Secured over-the-air update	Authenticated transactions between a cloud server and secured flash FOTA – only from an authenticated cloud location

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon tool to develop CRA applications – ModusToolbox™



ModusToolbox™ Software is a modern, extensible development environment for Infineon microcontrollers, offering tools, libraries, and runtime assets for a flexible and comprehensive development experience.

Development Tools

The ModusToolbox™ tools package includes programs for creating applications, managing components, configuring peripherals, and compiling, programming, and debugging.

Run-Time Software

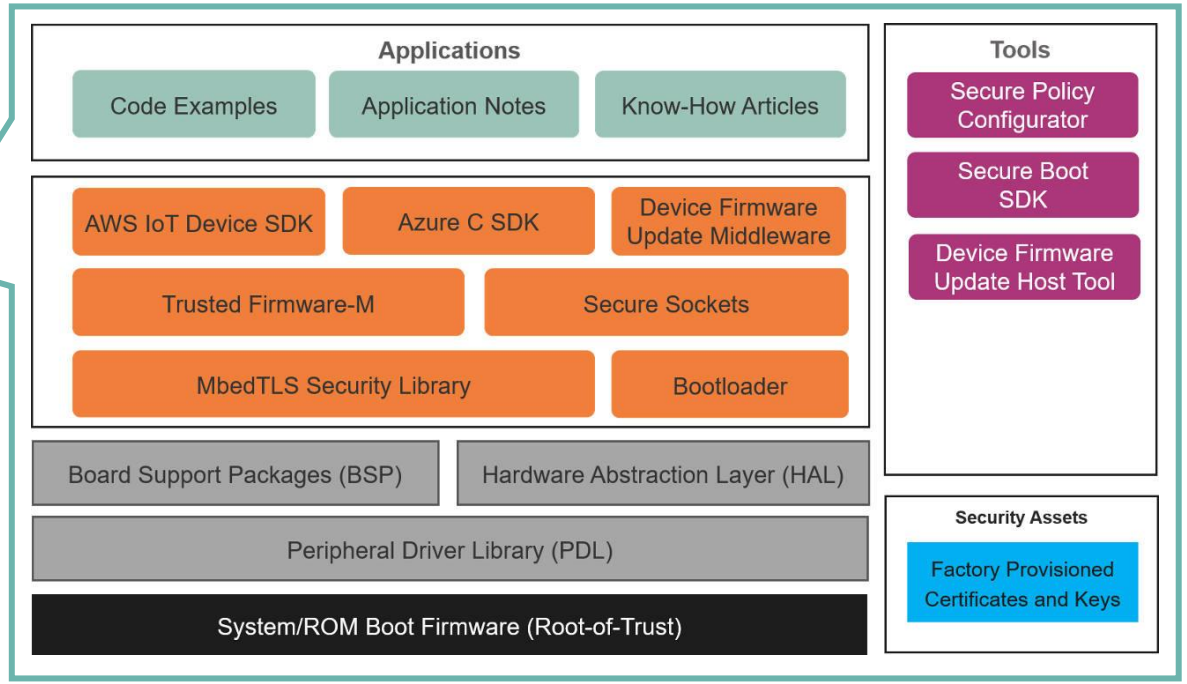
ModusToolbox™ software offers GitHub-hosted repositories with code examples, board support packages, middleware, and application support.

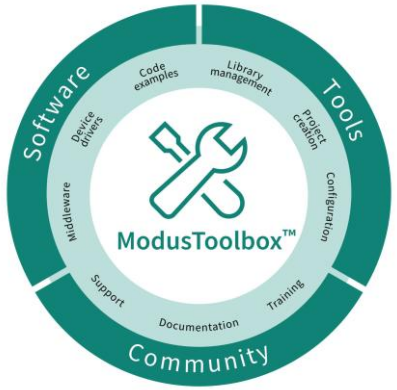
https://www.infineon.com/design-resources/development-tools/sdk/modustoolbox-software

Copyright © Infineon Technologies AG 2026. All rights reserved.

Software for Security

Software and Resources
ModusToolbox™ for security
ModusToolbox™ Edge Protect Security Suite
PSOC™ Edge E84 – Security Edge Protect Bootloader
Infineon OPTIGA™ Trust M overview repository
ModusToolbox™ examples for PSOC™ 6 security
OPTIGA™ Software and Tools





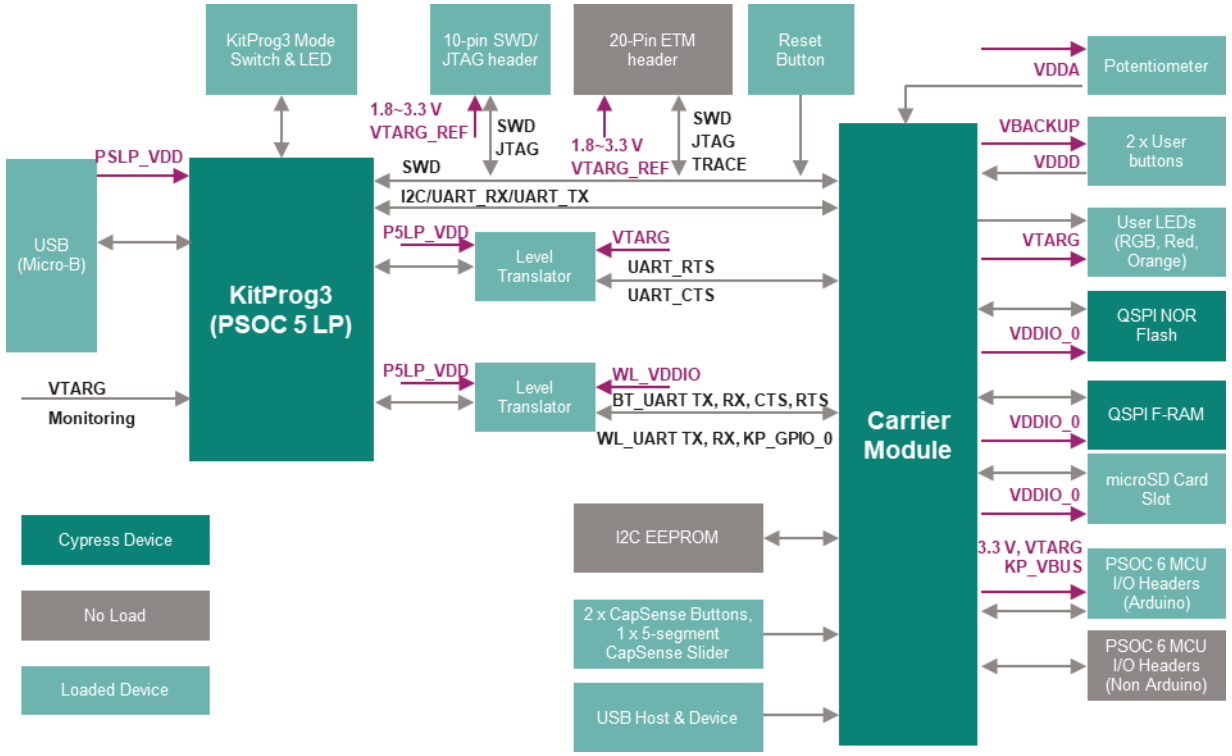


DEEPCRAFT™ Studio

Copyright © Infineon Technologies AG 2026. All rights reserved.

Reference Architecture – PSOC™ 6 WiFi-BT Pioneer Kit





Kit features

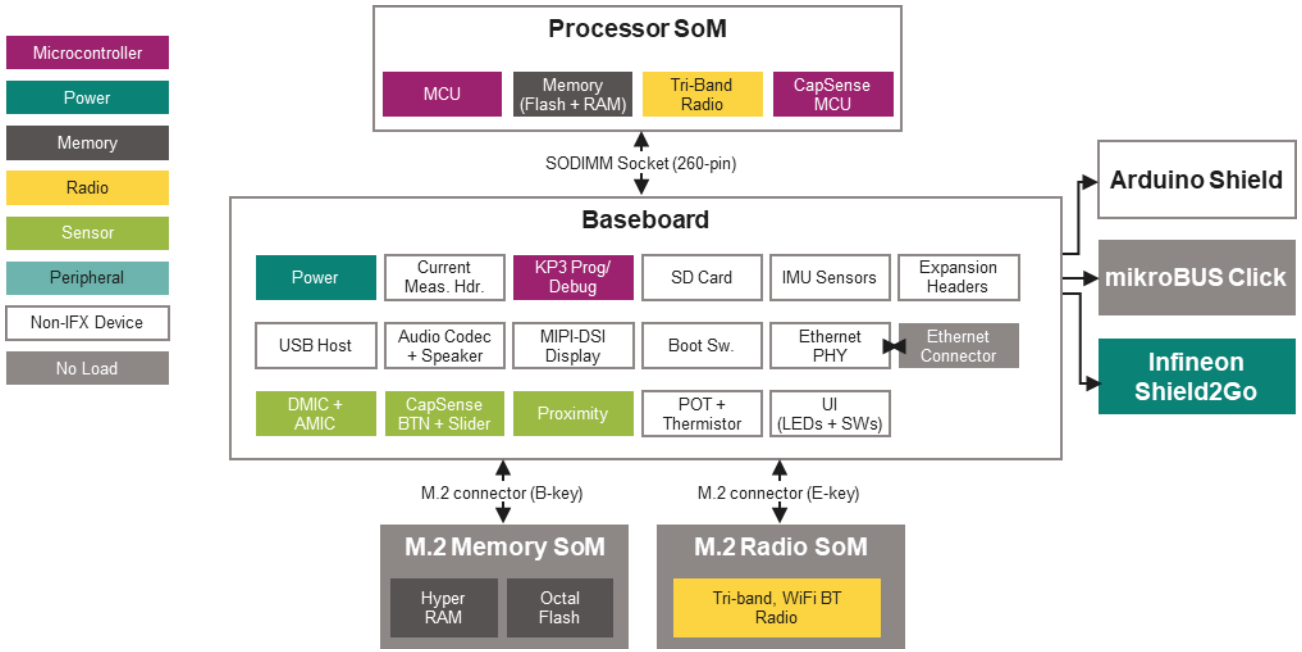
- **build EU CRA default class devices**
- Kit for: PSOC™ 624A, 6248, 61A, 6148
- Includes OPTIGA™ Trust-M security IC
- ModusToolbox™ software support
- Includes CYW43012 Wi-Fi/BLE combo radio
- Arduino Uno R3 header for Arduino shield
- CAPSENSE™ touch buttons and slider
- 512-Mbit external Quad-SPI NOR Flash
- 4-Mbit Quad-SPI F-RAM, microSD card I/F
- On board SWD, USB-UART, USB-I2C bridges
- USB device and host functionality
- User buttons, LEDs, potentiometer

Here's the link to PSOC™ 6 WiFi-BT Pioneer Kit

Copyright © Infineon Technologies AG 2026. All rights reserved.

Reference Architecture – PSOC™ Edge E84 Evaluation Kit





Kit features

- **build EU CRA default, important class device references**
- PSOC™ 4000T as CAPSENSE™ coprocessor
- Supported by ModusToolbox™ and DEEPCRAFT™ AI Suite
- Many code examples for security
- Onboard AIROC™ Wi-Fi & Bluetooth™ combo
- Analog and PDM microphones
- 6-axis accelerometer, gyroscope IMU, 3-axis magnetometer
- High speed interfaces, as Ethernet, USB
- MIPI-SI display interface
- KitProg3 onboard SWD programmer/debugger
- M.2(B-key) for external memory
- M.2(E-key) for radio connectivity modules

Here's the link to PSOC Edge E84 Evaluation Kits

Copyright © Infineon Technologies AG 2026. All rights reserved.

Infineon Solutions Block Diagram

Hyperlinks to Product Web Pages

#CROSS-SELLING LINK #DIGITALIZATION #DECARBONIZATION #Partner Ecosystems MyInfineon

Sensors

Current Sensors
Environmental (CO_2) Sensors
Magnetic Sensors
MEMS Microphones (XENSIV™)
Pressure Sensors
Radar & Image Sensors

Power

AC/DC Power Conversion
Buck Converters
Class D Audio Amplifiers
DC/DC Switching Regulator (PMIC)
OPTIREG™ LDOs
GAN (CoolGaN™) Transistors
Gate Driver ICs
High Power Diodes & Thyristors
Isolated Industrial Interface
Intelligent Power Modules (IPM)
LITIX™ LED Drivers
MOSFET/IGBT Modules
Motor Control ICs
Power Factor Correction
Solid State Relay
USB Type-C and Power Delivery
Wide Bandgap Semi's (SiC/GaN)

Analog/Discrete

IGBTs
Low-Side / High-Side Switches
MOSFETs
MOSFET/IGBT Drivers

Audio

Class D Audio Amplifiers
MEMS Microphones

Safety Solutions ASIL-D

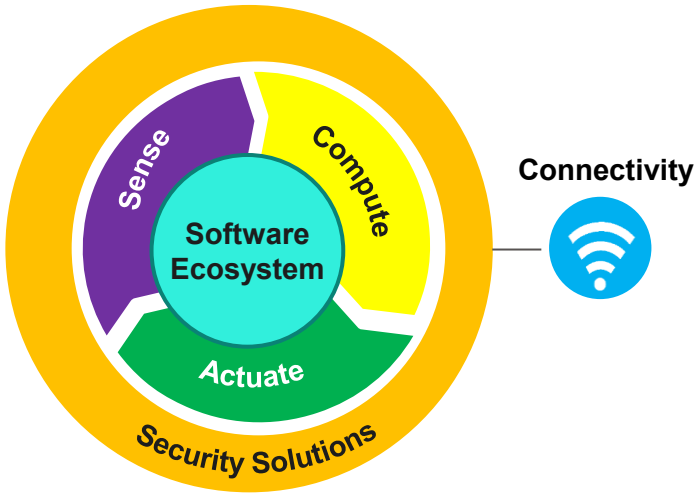
AURIX™ Safety Concept
Safety Products PRO-SIL™

Memory

NOR Flash / FRAM / HyperBus / SRAM/RRAM

Microcontrollers

AURIX™
PSOC™ 4
PSOC™ 6
PSOC™ Control
PSOC™ Edge
PSOC™ Multitouch
TRAVEO™ Automotive
32-bit XMC™ Arm® Cortex®- M



Actuate: Analog/Discretes, Motor Control, Power
Compute: Microcontrollers, Memory, Safety, ASIL-D
Connectivity: Wi-Fi, Bluetooth, Tranceivers, USB
Sense: Audio, Sensors
Security Solutions: Security / Smart Cards

RF & Wireless (Wi-Fi / BLE)

Antenna Centric Devices
High Reliability Discretes
Low Noise Amplifier LNA ICs
Radar Sensors XENSIV™
RF Transistors
RF Diodes
RF Switches (SPxT, DPxT)
RF Modules (LMM)
AIROC™ Wi-Fi + BLE Combos
Partner Connectivity Modules
AIROC™ BLE® & Multiprotocol
Wireless Control Receiver

I/O Interface / USB

Alternator Regulator
TRAVEO™ CAN FD
Constant Current Control IC
Engine Management IC
Smart Power Switches
Security/Authentication
System Basis Chips (SBC)
Universal Serial Bus (USB)

Wired Connectivity

Automotive Ethernet
Automotive Bridges
Automotive Phys
Automotive Switches
Automotive Transceivers
Industrial Transceivers

Security Solutions / Smart Cards

AURIX™ Security Solutions
CIPURSE™ Products
Contactless Memories
OPTIGA™ Embedded Security
SECORA™ Pay Security
Smart Cards for Government ID
Security Controllers
Security Controllers - USB Tokens
Smart Card Modules

Transistors & Diodes

ESD and Surge Protection

Motor Control

MOTIX™ | Embedded Power ICs
Low power BDC | BLDC motor drives
H-Bridge Driver IC with Integrated Arm® Cortex®
MOTIX™ | Multi Half-Bridge ICs
IGBTs
MOSFETs
IGBT Modules
Gate Driver ICs
Synchronous Rectifiers
MOTIX™ | Servo and Stepper Motor Driver

Table of contents

1 CRA vs. RED 4

2 CRA Compliance and Why Infineon 8

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 **Security Related Collaterals** **60**

7 Distribution Certification Program 66

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

Security Related App Notes/Whitepapers/Trainings (1)

Documents	Scope	Date Updated
PSOC™ Edge provisioning specification	How to enable provisioning of the PSOC™ Edge series of devices	Jun 7, 2024
How to meet the IoT security requirements of today and tomorrow	What governments suggests or requires and specific details on how to implement security defenses and obtain security certifications	July 2023
OPTIGA™ TPM - TPM Software OpenSource Eco System	why the TPM is favoured in the open source ecosystem and what resources we contribute for integrators and developers.	Sept 23, 2025
OPTIGA™ TPM Product Overview	Get an understanding of the OPTIGA™ TPM family	Oct 26, 2024
Enabling CRA compliance with Infineon: SEMPER™ Secure NOR Flash	How SEMPER™ Secure NOR Flash can help customers address the CRA requirements in the system	Sept 18, 2025
Enabling CRA compliance with Infineon security: PSOC™ Edge, Control family, Wi-Fi & BLE solutions	How OEMs should prepare for the CRA, the security benefits offered by Infineon, and how to address the four categories required by the CRA	Sept 11, 2025
Edge AI – Secured Intelligence Everywhere	How to create secure, efficient, and scalable solutions that will take your devices to the next level.	Sept 10, 2025
Trusted Computing Group (TCG) and Trusted Platform Module (TPM)	Overview of the Trusted Computing Group (TCG) organization and the technologies and standards (such as TPM) that it develops to enable secure computing	Nov 14, 2023
OPTIGA™ TPM Preparation Migration Guide	A TPM preparation guide to migrate from OPTIGA™ SLB9672/SLB9673 to SLB967x	Sept 23, 2025

Copyright © Infineon Technologies AG 2026. All rights reserved.

Security Related App Notes/Whitepapers/Trainings (2)

Documents	Scope	Date Updated
PSOC™ Edge E84 – Security Introduction	How the PSOC Edge security architecture can help achieving high security standards demanded by the industry	Apr 23, 2025
Introduction to Security Controllers	An overview of the key features of a security controller	Feb 10, 2025
OPTIGA™ Trust M–Security for Connected “IoT”	OPTIGA™ Trust M distribution certification program	May 7, 2021
Enabling CRA compliance with Infineon: USB Portfolio	The WCS portfolio and the specifically CRA relevant products Infineon offers	Sept 18, 2025
Securing the Edge: Building Secure Systems with PSOC™ Edge	Key security features of PSOC Edge	Oct 16, 2025
Security in Industrial Applications and Power Tools	Unique security challenges in industrial applications that can be addressed with the Infineon offering	Aug 6, 2024
Sales Training for OPTIGA™ Trust M MTR	OPTIGA™ Trust M Matter’s features, benefits, and real-world applications	Oct 24, 2023
Infineon's Infrastructural & Device Security	Distribution silver certification program	Sept 8, 2022
Getting started with PSOC™ 6 security	Basic security features implemented on PSoC™ 6 (61/62/63) devices	Mar 22, 2024
Getting started with PSOC™ 64 security	Security features in PSOC™ 64	Sept 11, 2024
ModusToolbox™ Training Collection	A series of trainings for getting started with and delving deeper into ModusToolbox™	Dec 17, 2024

Copyright © Infineon Technologies AG 2026. All rights reserved.

Security Related App Notes/Whitepapers/Trainings (3)

Documents	Scope	Date Updated
Sales and DFAE Training on the OPTIGA™ TPM	How the PSOC Edge security architecture can help achieving high security standards demanded by the industry	Apr 12, 2025
Update on Trusted Computing Group (TCG) and Trusted Platform Module (TPM)	Examples how the TCG and TPM enable trusted computing and why Infineon has been a strong contributor, are provided	Nov 18, 2025

Copyright © Infineon Technologies AG 2026. All rights reserved.

Application Presentations (1)

Application Presentations	Type	Date Created/Updated
CRA for DC EV Charging	Customer training	Oct 2025
Photovoltaic Inverter	MAPS2	Aug 25, 2025
Industrial Drives	MAPS2	Aug 25, 2025
Infineon Matter System Solutions	MAPS2	Aug 25, 2025
Security Camera and Video Doorbell	MAPS2	Aug 25, 2025
Alarm and Security Systems	MAPS2	Aug 25, 2025
AC EV Charging	MAPS2	Aug 25, 2025
Solar Inverter for Photovoltaic (PV) Panels	MAPS2	Aug 25, 2025
Smart thermostat	MAPS2	Aug 25, 2025
Diabetes Management	MAPS2	Aug 25, 2025
Electronic Shelf Labels	MAPS2	Aug 25, 2025
Smart Watch and Wristband	MAPS2	Aug 25, 2025
DC EV Charging	MAPS2	Aug 25, 2025

Copyright © Infineon Technologies AG 2026. All rights reserved.

Application Presentations (2)

Application Presentations	Type	Date Created/Updated
Home and Professional Cordless Power Tools	MAPS2	Aug 25, 2025
Solar Inverter for Photovoltaic (PV) Panels	MAPS2	Aug 25, 2025

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 CRA vs. RED 4

2 CRA Compliance and Why Infineon 8

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 **Distribution Certification Program** **66**

8 Key Takeaways 68

Copyright © Infineon Technologies AG 2026. All rights reserved.

Distribution Certification Program

Certification Program	Level	Length	Launch Date
Cyber Resilience Act (CRA): Foundations of Secure Solutions – Distribution FAE Certification Program	Silver	3h 25min	Oct 21, 2025
Cyber Resilience Act (CRA): Foundations of Secure Solutions – Distribution FAE Certification Program	Gold	3 days of onsite hands-on training	Jan 2026

These Certification Programs were designed specifically for our Distribution Partners, to extend the reach of Infineon's expertise through Distributors experts.
Obtaining Infineon's certificate proves deep knowledge and understanding of Infineon's solutions in this area.
Please contact our official, franchised Distribution Partners to get more information:
https://www.infineon.com/contact-us/where-to-buy?ftab=03

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 CRA vs. RED 4

2 CRA Compliance and Why Infineon 8

3 RED Compliance and Why Infineon 30

4 Infineon's Response to CRA/RED 36

5 Infineon Solution Compliant with CRA/RED 40

6 Security Related Collaterals 60

7 Distribution Certification Program 66

8 **Key Takeaways** **68**

Copyright © Infineon Technologies AG 2026. All rights reserved.

Key Takeaways

1. Infineon is leading in security expertise to support customers in their CRA compliance journey, covering broad applications
2. Infineon has been offering and continue to offer webinars, online training courses, technical collaterals on CRA/RED and support security by design
3. Infineon offers broad product portfolio and solutions in compliance with CRA/RED.
   Seek for Infineon's recommendation on selecting the right MCU to comply with CRA/RED
4. Adding a dSE (discrete Secure Element) can simplify manufacturing, improve efficiency, and save costs down the line
5. Contact our official, franchised Distribution Partners to receive the support from the experts certified by Infineon → https://www.infineon.com/contact-us/where-to-buy?ftab=03

Copyright © Infineon Technologies AG 2026. All rights reserved.


Infineon