EU Cyber Resilience Act (CRA)

Technical Guidance for Digital Products

About this document

This Application Note gives an overview on the EU – Cyber Resilience Act (CRA). It provides information on the motivation for the CRA, regulatory scope and timelines, manufacturer obligations, essential security requirements, documentation expectations, and the role of hardware security building blocks such as discrete Secure Elements (dSE), Wi-Fi, BT, Wi-Fi/BT Combo and MCU.
Note: Currently this document is focused on products and solutions with focus on connected secured systems. This document will be updated and extended regularly with latest information. Please crosscheck accordingly for newer versions on the Infineon website.

CRA Compliance Notice

References to Infineon products, security features, reference designs, examples and assessment packages are intended solely to illustrate potential contributions towards cybersecurity objectives. The use of an Infineon product or solution does not by itself establish compliance with the EU Cyber Resilience Act (CRA). Compliance must be assessed by the manufacturer of the final product based on the specific implementation, intended use and applicable regulatory requirements.

Scope and purpose

Provide engineers and product leaders with guidance to target CRA compliance activities across the full product lifecycle—from concept and risk analysis to secured development, vulnerability handling, incident reporting, documentation, and CE marking.

Intended audience

Hardware and software design engineers, security architects, technical program managers, product owners, quality & compliance engineers, and documentation specialists working on connected products and digital components.

Keypoints

• CRA shall apply to products with digital elements and shall establish mandatory security and vulnerability-handling requirements.
• Manufacturers bear responsibility for risk assessment, security-by-design, incident reporting, and lifecycle support.
• Transition periods: incident reporting obligations start earlier than full product compliance.
• Harmonized European Norms (hENs) by CENELEC will translate high-level legal obligations into technical measures.
• Discrete Secure Elements (e.g.,OPTIGA™ TPM/SECORA™) can offload cryptography and key storage, easing certification and compliance.
• In relation to the CRA requirements, this document will also cover security requirements and compliance considerations for embedded wireless components, including MCU, Wi-Fi, and Bluetooth module.

About CRA

The EU Cyber Resilience Act (CRA) is a regulation intending that products with digital elements—including connected hardware, software, and IoT devices—placed on the EU market meet a baseline level of

cybersecurity throughout their entire lifecycle. It introduces requirements for security-by-design and security-by-default development, mandatory vulnerability handling and reporting, and ongoing security updates for as long as the product is maintained.

Main Motivation

Explosive growth of connected devices:

- The number of internet connected devices is increasing rapidly.
  According to an industry forecast, the number of IoT-connected devices worldwide will rise from 13.2 billion in 2022 to 34.7 billion by 2028—more than doubling in just six years.
- The number of vulnerabilities and cyberattacks is reportedly rising
- More connected products can lead to a larger attack surface: Consumers may increasingly fall victim to security flaws in everyday digital products (e.g., cameras, routers, smart appliances).
- According to EU cybersecurity threat landscape analyses and industry reports, ransomware attacks have risen sharply, with estimates of one attack every ~11 seconds in 2020 and projections pointing to one every 2 seconds in the coming decade. [2]

These trends highlight the need for consistent, enforceable cybersecurity standards, which the CRA starts with.

Table of contents

About this document **1**
About CRA **1**
Table of contents **3**
1 CRA Overview **4**
2 Scope and applicability **5**
3 Timeline and transition periods **6**
4 CRA Manufacturer obligations across the lifecycle **7**
4.1 CRA Design & Development phase (pre-market) obligations: 7
4.2 CRA Maintenance phase (post-market) obligations: 8
4.3 CRA Reporting obligations 8
5 CRA Essential security requirements **10**
5.1 Part I: Product related cybersecurity requirements 10
5.2 Part II: Vulnerability handling requirements 11
5.3 Part III: Incident Report 11
6 CRA Documentation Requirements **12**
6.1 Documentation delivered to customers 12
6.2 Technical documentation (not delivered to customers) 12
7 Harmonized European Norms (hENs) **14**
8 Essential Requirements vs. Harmonized European Norm **15**
9 Different digital product categories and requirements **16**
10 BT, Wi-Fi, and MCU products bring benefit beyond security **17**
11 A discrete Secure Element brings benefits beyond security **18**
12 Risk Analysis Model for CRA – How a discrete Secured Element can enable for fast CRA compliance **19**
12.1 What is risk analysis? 19
12.2 How relevant is risk analysis for CRA? 21
12.3 Example risk analysis for wearables 22
13 How Infineon can help with CRA compliance **24**
14 Example of how Infineon can support with CRA compliance: Wi-Fi, BT, Wi-Fi/BT Combo, and MCU **25**
15 Example of how Infineon can support with CRA compliance: OPTIGA™ TPM **26**
16 Example of how Infineon can support with CRA compliance: SECORA™ Connect X **28**
17 Infineon Edge Systems portfolio broadly supports CRA security regulations **30**
18 References **33**
Revision history **34**
Disclaimer **35**

1 CRA Overview

The Cyber Resilience Act (CRA) establishes uniform cybersecurity requirements for products with digital elements that are made available on the European Union market. It lays down essential cybersecurity requirements that must be fulfilled before a product is placed on the market, as well as ongoing obligations that apply once the product has been made available within the Union.

The CRA was introduced in response to the growing number of cybersecurity vulnerabilities and incidents linked to connected hardware and software products placed on the EU market. A growing attack surface, increasing device counts, and the persistence of exploitable flaws prompted the EU to set a common security baseline for digital products.

Under the CRA, manufacturers must foster that products comply with the essential cybersecurity requirements prior to placing them on the market. These requirements address secured design and development, protection against unauthorized access, safeguarding of confidentiality, integrity and availability, and the establishment of vulnerability handling processes.

In addition to pre-market compliance obligations, the Regulation includes post-market duties, including vulnerability monitoring, provision of security updates during the declared support period, and reporting of actively exploited vulnerabilities and severe incidents. Economic operators must also follow conformity assessment procedures and affix CE marking to demonstrate compliance.

2 Scope and applicability

The CRA applies to complete devices (e.g. smartphones, wearables) as well as embedded components (e.g. microcontrollers, sensors), and standalone software that can connect directly or indirectly to the internet. Non-commercial projects and cloud-only services are out of scope.

Compliance and Fines

- For non-compliance or misleading information, the regulation provides for penalties like:
  - Fines up to €15M, €10M, or €5M, or
  - Up to 2.5%, 2%, or 1% of global annual turnover (whichever is higher)
- Possible enforcement actions: fixing issues or recalling products
- Enforcement may occur through random sampling by ENISA or, under competition law, by competitors.

3 Timeline and transition periods

The Cyber Resilience Act (CRA) entered into force in October 2024, providing a 36-month transition period before its full application. During this period, vulnerability and incident reporting obligations will apply 21 months after its entry into force, and the product compliance obligation is scheduled to commence in December 2027.



DISCLAIMER: The timeline is a rough estimate

Figure 1 Timeline and transition period

4 CRA Manufacturer obligations across the lifecycle

Article 13 and 14 of the CRA sets out comprehensive obligations for manufacturers of products with digital elements. Below is a summary of the key requirements.

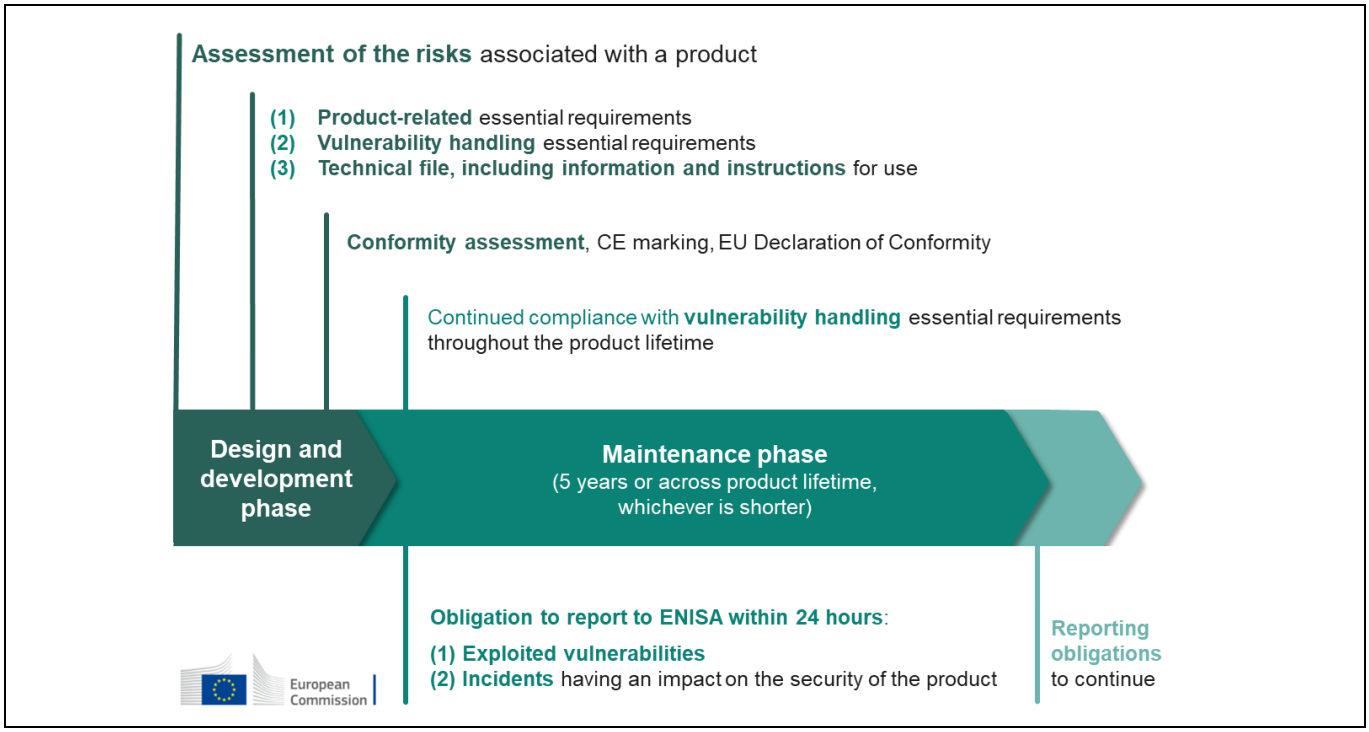


Figure 2 Manufacturer obligations

4.1 CRA Design & Development phase (pre-market) obligations:

The manufacturer has several obligations before placing a product with digital element on the market:

- Design, develop, and produce products with digital elements in accordance with essential cybersecurity requirements
- Conduct a cybersecurity risk assessment to minimize risks, prevent incidents, and protect user health and safety
- Documentation and updates of the risk assessment during the product's support period, considering factors like intended use, operational environment, and asset protection
- Include the risk assessment in the technical documentation and provide a clear justification if certain requirements are not applicable
- Exercise due diligence when integrating third-party components, including open-source software, to check they do not compromise the product's cybersecurity

- Report vulnerabilities in components to the component manufacturer and address them according to Annex I requirements
- Share modifications to address vulnerabilities with the component manufacturer in a machine-readable format
- Document cybersecurity aspects, including vulnerabilities, and update the risk assessment as needed
- Foster effective vulnerability handling for products with digital elements during the support period, in accordance with Annex I requirements
- Once compliance with the essential cybersecurity requirements has been demonstrated, manufacturers draw up a EU Declaration of Conformity and affix the CE marking to the product, indicating that it meets the necessary standards and is authorized for sale within the European Union

4.2 CRA Maintenance phase (post-market) obligations:

- Manufacturer must safeguard that security updates as well as the technical documentation are available for at least 10 years after the product has been placed on the market or for the full support period, whichever is longer
- Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources

4.3 CRA Reporting obligations

Article 14 of the CRA establishes mandatory reporting obligations for manufacturers. Manufacturers must report actively exploited vulnerabilities as well as severe cybersecurity incidents in their products with digital elements upon becoming aware of them simultaneously to CSIRT and ENISA.

Manufacturers must notify authorities of actively exploited vulnerability in their product with digital element within the following timelines:

- Early warning notification within 24 hours, indicating, where applicable, the Member States on the territory their product has been made available
- Vulnerability notification within 72 hours, providing general information about the product, exploit, and vulnerability, as well as corrective measures
- Final report within 14 days of a corrective measure being available, including details about the vulnerability, severity, impact, and security updates

Manufacturers must report severe actively exploited incidents impacting the security of their products with digital elements to within the following timelines:

- Early warning notification within 24 hours, including whether the incident is suspected to be caused by unlawful or malicious acts

- Incident notification within 72 hours, providing general information about the incident, initial assessment, and corrective measures
- Final report within one month, including a detailed description of the incident, its severity and impact, root cause, and mitigation measures

Severe Incident Criteria:

An incident is considered severe if it:

- Negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions.
- It has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements

Severe incidents having an impact on the security of the product with digital elements, on the other hand, refer to situations where a cybersecurity incident affects the development, production or maintenance processes of the manufacturer in such a way that it could result in an increased cybersecurity risk for users or other persons. Such a severe incident could include a situation where an attacker has successfully introduced malicious code into the release channel via which the manufacturer releases security updates to users.

5 CRA Essential security requirements

Annex I of the CRA outlines two categories of cybersecurity requirements: Part I focuses on the properties of products with digital elements and Part II defines requirements for vulnerability handling and lifecycle management.

5.1 Part I: Product related cybersecurity requirements

1. Products with digital elements shall be designed, developed and produced in such a way that they realize an appropriate level of cybersecurity based on the risks
2. On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
   - be made available on the market without known exploitable vulnerabilities
   - have a secured default configuration, with optional reset to original state
   - vulnerabilities can be addressed through security updates, including automatic updates with opt-out mechanisms
   - protect against unauthorized access using control mechanisms like authentication and access management and report on potential breaches
   - protect data confidentiality through encryption and other technical means, for both stored and transmitted data
   - protect data integrity against unauthorized manipulation or modification and report on corruptions
   - process only data that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization)
   - protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks
   - minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks
   - be designed, developed and produced to limit attack surfaces, including external interfaces
   - be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques
   - provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user
   - provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, foster that this is done in a secured manner

5.2 Part II: Vulnerability handling requirements

Manufacturers of products with digital elements shall:

- Identify and document vulnerabilities and components in products with digital elements, including a software bill of materials
- Address and remediate vulnerabilities promptly, including providing security updates
- Conduct regular tests and reviews of product security
- Share information about fixed vulnerabilities, including descriptions and remediation guidance
- Establish a policy on coordinated vulnerability disclosure
- Facilitate sharing of vulnerability information, including a contact address for reporting
- Allow secured distribution of updates to fix or mitigate vulnerabilities
- Offer security updates promptly, with advisory messages providing relevant information

5.3 Part III: Incident Report

Manufacturers need processes for managing **vulnerabilities** and addressing 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.

6 CRA Documentation Requirements

6.1 Documentation delivered to customers

At minimum, the product with digital elements shall be accompanied by the following information and instructions and to the user:

- manufacturer name/trade name/trademark and contact details (postal address plus email/other digital contact, and website where available)
- a single point of contact for vulnerability reporting/receipt and access to the coordinated vulnerability disclosure policy
- product name/type and information enabling unique identification
- intended purpose, provided security environment, essential functionalities, and security properties
- known or foreseeable use or reasonably foreseeable misuse circumstances that could lead to significant cybersecurity risks;
- where applicable, the internet address for the EU declaration of conformity
- the type of technical security support and the support end-date for vulnerability handling and security updates
- instructions or a link to instructions on secured commissioning and use throughout the product lifetime, security impacts of changes, installing security updates, secured decommissioning and data removal, how to switch off automatic security updates, and—if intended for integration—information needed for integrators to meet Annex I and Annex VII requirements
- if provided, where to access the software bill of materials.

6.2 Technical documentation (not delivered to customers)

For internal documentation manufacturers must maintain a technical dossier with risk assessment, applied standards, design/manufacture locations, conformity assessment procedure, labels and instructions, test results, declaration of conformity (DoC), and support period information. Instructions should include secured commissioning/decommissioning, update procedures, and—if applicable—the public location of the SBOM.

The technical documentation for a product with digital elements must include the following information:

- A general description of the product, including its intended purpose, software versions, and user information
- Details on design, development, and production, such as system architecture, vulnerability handling processes, and software bill of materials
- An assessment of cybersecurity risks and how the product meets essential cybersecurity requirements
- Information on the support period and relevant considerations
- A list of applied harmonized standards, common specifications, or European cybersecurity certification schemes, and descriptions of alternative solutions if these were not applied

- Test reports verifying conformity with essential cybersecurity requirements
- A copy of the EU declaration of conformity
- The software bill of materials, if requested by a market surveillance authority for compliance checking

7 Harmonized European Norms (hENs)

CENELEC is developing hENs to provide presumption of conformity when applied. Process standards will cover vulnerability handling and incident reporting; product standards translate essential requirements into concrete technical measures (e.g., cryptographic protocols, secured update, logging). Drafts are expected before full product-compliance obligations take effect.

8 Essential Requirements vs. Harmonized European Norm

Table 1 Aspects Essential Requirements vs. Harmonized European Norm

Aspect	CRA Essential Requirements	Harmonized Standards (hENs)
Nature	Legal, high-level obligations	Technical, practical guidance
Focus	Defines what must be achieved	Defines how to achieve it
Level of detail	High-level, principle based, e.g. “Product must protect data”	Detailed, specific technical solutions, e.g. “Use TLS v1.2+ for encrypting data in transit”
Mandatory / Optional	Mandatory	Optional (grants presumption of conformity)
Developed by	EU Legislator (EU commission)	Standard bodies (CEN, CENELEC, ETSI)
Usage	All products in scope	Recommended for compliance

9 Different digital product categories and requirements

The CRA defines three main product categories for regulatory purposes. These come from Articles 7 and 8 together with Annex III (Important products) and Annex IV (Critical products)— the official lists of higher-risk products with digital elements[1].

1. Default “Class 0”

   All products with digital elements that are not listed in Annex III or IV.

   Examples:

   - Smart TVs
   - Monitors
   - Speakers

2. Important Products

   Annex III lists products whose core functionality places them in the “Important” category. It is divided into:

   - Class I

     Includes product categories such as:

     - Internet routers, modems and switches
     - Microprocessors and microcontrollers with security related functionality
     - Secured ASICs and FPGAs
     - Smart home products like voice assistants, security devices (locks, cameras, alarms)
     - Smart toys with interactive or tracking features
     - Health and child-tracking wearables

   - Class II

     Includes product categories such as:

     - Tamper resistant micro processor
     - Tamper resistant microcontroller

3. Critical Products

   Annex IV lists products considered critical due to systemic cybersecurity impact. Examples include:

   - Smart meter gateways and other devices built for advanced security like secured data processing.
   - Smartcards and similar secured chips (like secured elements used in payment cards or SIM cards).

[1] Please note that the shown lists in this chapter are only an excerpt of the full list.

10 BT, Wi-Fi, and MCU products bring benefit beyond security

In today's IoT landscape, Wi-Fi, Bluetooth, Wi-Fi/BT combo, and MCU products go far beyond simple connectivity — they come equipped with **built-in security capabilities**. These products are classified under the **Edge Protect Category (EPC)** framework, ranging from EPC1 to EPC4, each delivering distinct levels of performance and security functionality.

EPC1 represents the baseline security tier, supporting **CRA Default/Class 1** compliance. It provides accelerated cryptography, secured boot, secured firmware updates, processing isolation, and boot-time physical fault attack mitigation. All product families — Wi-Fi, BT, combo, and MCU — can meet fundamental security requirements at this level.

EPC2 adds additional wireless connectivity security services, maintaining **CRA Class 1** compliance. Beyond EPC1 features, it introduces a **prebuilt security stack**, significantly reducing implementation complexity for Wi-Fi and BT-connected devices, allowing manufacturers to deploy proven security features without building them from scratch.

EPC3 delivers hardened accelerated cryptography with fault and glitch mitigation, meeting **CRA Class II** requirements. It extends physical fault attack mitigation to **both boot-time and runtime**, and adds a fault sensor management system along with DICE-ready SPDM support for stronger device authentication and secure communication.

EPC4 represents the pinnacle of security, featuring a hardware-isolated, lockstep Secure Enclave supporting **CRA Class II**. With advanced accelerated cryptography and complete hardware isolation, it is purpose-built for the most demanding applications in industrial, medical, and smart infrastructure environments.

Through the EPC framework, Wi-Fi, BT, Wi-Fi/BT combo, and MCU product families enable manufacturers to select the **optimal security solution** aligned with their application requirements, for efficient compliance with international regulations such as the CRA.

Edge Protect Category (EPC) #		EPC 1	EPC 2	EPC 3	EPC 4
Definition and Compliance		Minimum ICW MCU requirements SESIP L1, PSA L1v2	Additional wireless connectivity security services SESIP L2, PSA L2	Hardened accelerated crypto and fault, glitch mitigation SESIP L3, PSA L3	Hardware isolated, lockstep Secure Enclave (SE) SESIP L3, PSA L3+PSA L4 iSE
Features	CRA/RED support	✓ Class 1	✓ Class 1	✓ Class 2	✓ Class 2
	Cryptography	✓ Accelerated	✓ Accelerated	✓ Hardened Accelerated	✓ Advanced Accelerated
	Secured boot	✓	✓	✓	✓
	Secured FW update	✓	✓	✓	✓
	Processing isolation	✓	✓	✓	✓
	Physical fault attack mitigation	✓ Boot-Time	✓ Boot-Time	✓ Boot-Time/Run-Time	✓ Boot-Time/Run-Time
	Prebuilt security stack available		✓	✓	✓
	Fault sensor management system			✓	✓
	DICE support for SPDM			✓ DICE Ready	✓
	Hardware isolated secure enclave				✓

Figure 3 Edge Protect Categories

11 A discrete Secure Element brings benefits beyond security

MCUs may lack memory and performance to meet CRA requirements. CRA demands robust security features such as secured boot, cryptographic operations, secured firmware updates, and continuous vulnerability monitoring. Implementing these features on a traditional MCU can quickly exhaust available resources, leading to performance bottlenecks and design limitations.

Solution: Offload security functions to a discrete Secured Element (dSE). A discrete Secure Element (dSE) addresses these challenges by providing a dedicated, isolated security processor that handles security-critical operations independently from the main MCU. This architecture offers several key advantages like:

Performance optimization: The dSE includes hardware-accelerated cryptographic engines, delivering significantly faster performance than software implementations on general-purpose MCUs.

Isolated secured storage: The dSE provides dedicated non-volatile memory for storing sensitive data such as cryptographic keys, certificates, and security configurations, freeing up valuable MCU memory.

Implementation cost and effort depend on the required security level. Achieving CRA compliance through traditional MCU-based security implementations can be resource-intensive, requiring significant investment in development, testing, certification, and ongoing maintenance. The total cost of ownership extends far beyond the initial component price, encompassing engineering effort, time-to-market delays, certification expenses, and lifecycle management costs.

Solution: A discrete Secured Element simplifies design and reduces total cost of ownership. dSEs come with a complete, tested security software stack including cryptographic libraries, secured boot implementations, key management systems, and secured communication protocols. This eliminates the need for manufacturers to develop these complex components from scratch, saving months of specialized development effort.

CRA encourages unique device identities using keys and certificates. This emphasis is rooted in the fundamental security principle that every connected device must be uniquely identifiable, authenticatable throughout its lifecycle.

Solution: dSE enables wafer-level provisioning of customer keys and certificates for Zero-Touch Provisioning (ZTP). This creates a secured hardware-bound identity that is protected from being replicated, cloned, or transferred to another device, providing a strong foundation for device identity.

12 Risk Analysis Model for CRA – How a discrete Secured Element can enable for fast CRA compliance

12.1 What is risk analysis?

Cyber Risk Analysis: Documenting Security Risks

- Cyber risk analysis is the structured practice of:
    - identifying assets and security objectives (e.g., confidentiality of keys, integrity of firmware),
    - identifying threats and vulnerabilities,
    - estimating likelihood and impact,
    - mitigations based on quantified or ranked risk.
- For device ecosystems (IoT, terminals, embedded), the “asset” is often something like device identity, cryptographic keys, firmware integrity, or sensor/transaction data.

Risk calculation

Use the stated formula:

- Risk = P(Threat) × P(Vulnerability)
    - Where:
        - P(Threat) between [0,1]: likelihood that a relevant threat event/actor will attempt the attack (e.g., remote attacker targeting fleet devices; supply-chain attacker; local physical attacker).
        - P(Vulnerability) between [0,1]: likelihood the device/system can be successfully exploited given the attempt (e.g., key extraction possible; compromised boot; debug interface exposed).
- This yields a risk score between [0,1].

Threshold-based decision rule

Define a risk threshold (example: 0.6).
If:

- Risk > 0.6 → action required
- This threshold represents your “unacceptable risk” line. Anything above it must be reduced (mitigated), transferred, avoided, or formally accepted with justification.

12 Risk Analysis Model for CRA – How a discrete Secured Element can enable for fast CRA compliance

Documenting a risk entry

For each risk, record:

- Asset: what you're protecting (e.g., device private key)
- Threat scenario: who does what (e.g., attacker extracts key to clone devices)
- Vulnerability: what enables it (e.g., keys stored in MCU flash)
- P(Threat): numeric estimate with rationale
- P(Vulnerability): numeric estimate with rationale
- Risk score: product of the two
- Threshold comparison: above/below 0.6 (as example)
- Countermeasures: what reduces P(Threat) and/or P(Vulnerability)
- Residual risk: recompute after controls
- Owner / due date / status: accountability

Countermeasure: Discrete Secured Elements

A discrete Secured Element (SE) is a dedicated hardware security component (separate chip/module) designed to protect secrets and perform sensitive operations in a tamper-resistant manner.

In device risk terms, SEs primarily reduce P(Vulnerability) for classes of attacks like:

- key extraction (keys are not exposed to main MCU memory)
- credential cloning (hardware-backed identity)
- firmware authenticity bypass (secured boot / signed update validation with protected keys)
- secured authentication (challenge–response using protected private keys)

They're "practical" because they can often be integrated without redesigning the entire system security model, and they provide a clear reduction in exploitability for high-value assets.

12.2 How relevant is risk analysis for CRA?

CRA is effectively mandatory per product (device/product type).

Under the EU Cyber Resilience Act, manufacturers must perform cybersecurity risk assessment/risk management for each product with digital elements they place on the market, because the required security measures must be appropriate to that product's risks. You can't do one generic assessment for the whole company and be compliant.

You can reuse a common method and shared threat models across similar devices/platforms.

But you still need a product-specific assessment (or a clearly defined product family) that reflects that device's intended use, interfaces, exposure, and deployment context, and you must keep it updated over the lifecycle.

Risk analysis is important for the CRA because the Act is built around the idea that cybersecurity measures must be **appropriate to the risks** of the specific product. Without risk analysis, you can't credibly show that what you implemented is necessary, sufficient, and proportionate.

12.3 Example risk analysis for wearables

Table 2 Wearables: Usecase, Assets, Threats, Countermeasures

Wearables	**Focus: Smart ring & Accessories**
Usecase	• UC Payment Transactions • UC Tokenization • UC Physical Access • UC Logical Access • UC OS / Applet / Keys Update (in field) • UC Secure Communication • UC Mobile Drivers License • UC Transport / Ticketing • UC Health Tracking • UC AI IP Protection • UC Life Cycle Management • UC Multi-Tenant Env
Asset	• SecCred.Pay • SecCred.DSEM.Tok • Cert.DSEM.Tok • SecCred&Data.Tok • Aliro.SecCred.PhysAccess • AccessProfile.PhysAccess • Fido.SecCred.LogicAccess • AccessProfile.LogicalAccess • Keys.SecCred.Update • Keys.SecCred.Comm • Data&SeCred.MDL • Keys.Sym&RndN.TT • PersonalData.HT • SecCred.AI_IP • State.LifeCyc
Threats	Risk of: • Data and/or SecCred may be read or manipulated by an attacker • Computational logic manipulation • Availability (DoS) • Eavesdropping

Wearables	**Focus: Smart ring & Accessories**
	• Side-Channel attacks
Countermeasure	• Secured Storage with physical & logical readout protection incl. asset remains on the security chip • Secured Storage with physical & logical protection against manipulation • Crypto algorithms on chip incl. attack protection against probing, side channel and fault attacks • Secured generation and deployment of Keys

13 How Infineon can help with CRA compliance

Infineon's products play a crucial role in helping manufacturers achieve compliance with the CRA by acting as a hardware root of trust that enhances the overall security of the final product and minimizes regulatory risks. Our products enable the practical implementation of essential requirements outlined in Annex I, such as security-by-design principles. For instance, Infineon provisions keys and certificates at our secured, Common Criteria-certified facility. Additionally, our products undergo rigorous evaluation and certification according to industry standards like SESIP and PSA and are supported by specialized software tools and platforms that streamline secured development.

Infineon supports manufacturers throughout the security lifecycle of their products, starting from risk assessment over the product conformity assessment to vulnerability management and reporting. It offers educational resources, such as webinars, to help customers prepare for and comply with the EU's Cybersecurity Regulation (CRA).

Furthermore, Infineon's solutions provide additional benefits, including:

- **Reduced time-to-market**: By leveraging Infineon's pre-certified and pre-validated solutions, manufacturers can accelerate their product development and certification process, reducing the time and costs associated with compliance. **Improved supply chain security**: Infineon's secured provisioning and authentication mechanisms help to enforce the integrity of the supply chain, preventing counterfeiting and unauthorized modifications.
- **Access to expertise**: With over a decade of experience and in-depth knowledge of regulatory requirements, Infineon is well-equipped to guide manufacturers through the complex process of CRA compliance, targeting necessary standards and regulations.

14 Example of how Infineon can support with CRA compliance: Wi-Fi, BT, Wi-Fi/BT Combo, and MCU

Table 3 Wi-Fi, BT, Wi-Fi/BT Combo, and MCU as example for contribution towards product-related essential requirements

Product-related essential requirements	Wi-Fi, BT, Wi-Fi/BT Combo, and MCU
Appropriate level of security	AIROC™, PSOC™ Edge/Control, XMC™ device PSA security certification
Products to be delivered without known vulnerability	
Based on the risk and where applicable	
1. Security by default	Common Criteria, PSA Certified*, SESIP, IoT security standards such as ETSI EN 303 645, IEC 62443 and EN 18031 (ref. Radio Equipment Directive)
2. Protection from unauthorized access	Authenticated access, physical tamper resistance, secured connection, secured key storage/management, transport protection
3. Confidentiality and integrity of data, commands and programs	Confidentiality and integrity for keys/operations-supports lightweight integrity checks.
4. Minimization of data	Threat modeling e.g. PEN testing, SSC
5. Availability of essential functions	Service continuity, resilience & recovery, resource management, OTA update
6. Minimize own negative impact on other devices	Prevention of harmful interference and follow Radio Equipment Directives mandates.
7. Limit attack surfaces	Secured debug interfaces, passive security features (e.g. sensors, memory encryption), security critical information firewalled from processing environment
8. Reduce impact of an incident	All Wireless/MCU can be used to mitigate risk in SW layers e.g., side channel attack mitigation.
9. Record and monitor security relevant events	Wireless/MCU can be used for system / platform logs
10. Enable adequate security updates	Wireless/MCU can be used for secured communication with the back end for system / platform FW updates.

15 Example of how Infineon can support with CRA compliance: OPTIGA™ TPM

This chapter will denote the OPTIGA™ TPM as an example, how OPTIGA™ TPM enables product related essential requirements

Table 4 OPTIGA™ TPM as example for contribution towards product-related essential requirements

Product-related essential requirements	OPTIGA™ TPM
Appropriate level of security	OPTIGA™ TPM is CC EAL4+ certified.
Products to be delivered without known vulnerability	
Based on the risk and where applicable	
11. Security by default	OPTIGA™ TPM is used with FIDO Device Onboarding for provisioning. OPTIGA™ TPM allows measured boot for integrity of the installed SW.
12. Protection from unauthorized access	OPTIGA™ TPM is used as an Authenticator with master password-based systems.
13. Confidentiality and integrity of data, commands and programs	OPTIGA™ TPM allows measured boot for system/platform integrity. It allows secured storage of system/platform data and secrets.
14. Minimization of data	
15. Availability of essential functions	
16. Minimize own negative impact on other devices	
17. Limit attack surfaces	System/platform security operations like key storage, crypto, certificate storage etc., can be offloaded to the OPTIGA™ TPM instead of operating them in the main MCU/MPU with an increased attack surface
18. Reduce impact of an incident	OPTIGA™ TPM can be used to mitigate risk in SW layers e.g., attacks on SW
19. Record and monitor security relevant events	OPTIGA™ TPM can be used for system / platform logs
20. Enable adequate security updates	OPTIGA™ TPM can be used for secured communication with the back end for system / platform FW updates.

15 Example of how Infineon can support with CRA compliance: OPTIGA™ TPM

- Network equipment contains valuable assets which need to be protected: users keys, firmware, Wi-Fi Credentials, etc.
- Those devices are connected to internet and may be easy to be poisoned by malware, creating botnets and DDoS attacks.
- New network architectures like Software Defined Networks (SDNs) introduces APIs and extra communication layers which may be entry points for attackers.

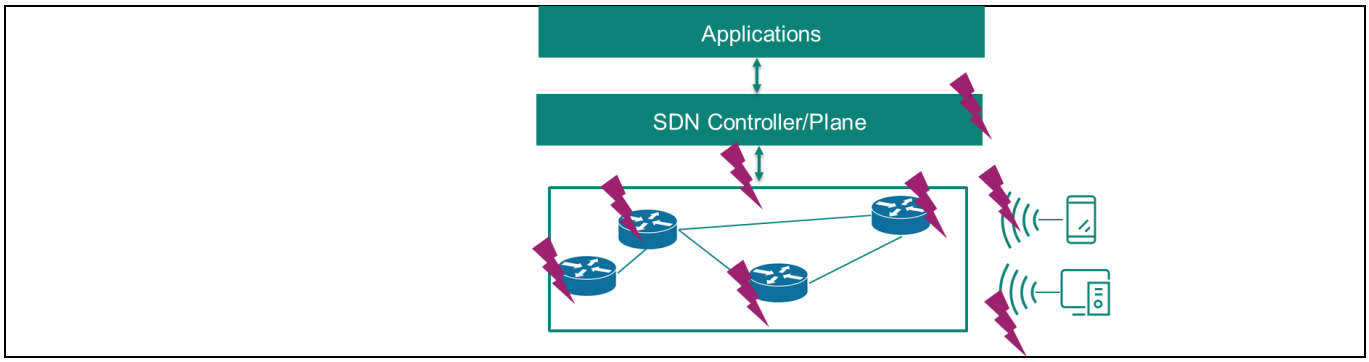


Figure 4 Application example for OPTIGA™ TPM in network equipment

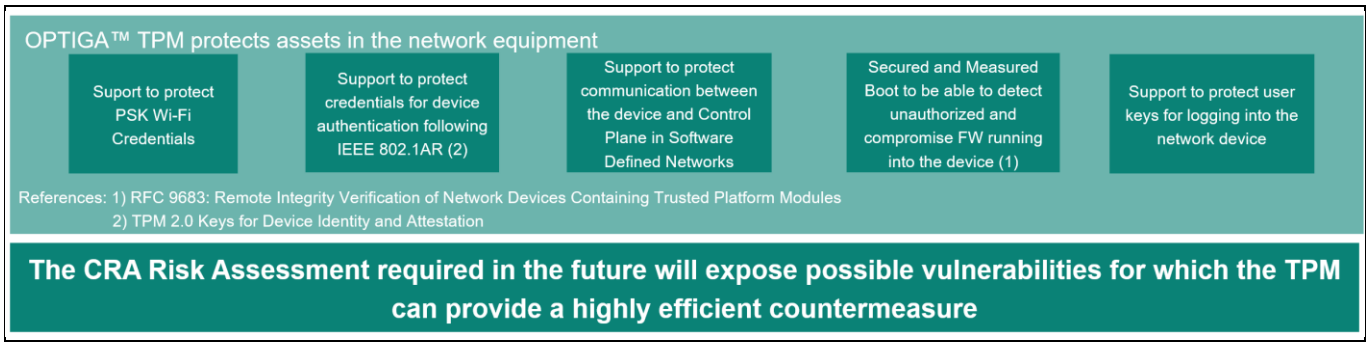


Figure 5 OPTIGA™ TPM mapping

16 Example of how Infineon can support with CRA compliance: SECORA™ Connect X

In the rather simple ring application, nearly all payment-relevant security is handled by the embedded NFC Secured Element.

Table 5 SECORA™ Connect X as example for contribution towards product-related essential requirements

Product-related essential requirements	SECORA™ Connect X
Appropriate level of security	SECORA™ Connect X helps to fulfill security requirement standards thanks to EMVCo certification which is equivalent to **Common Criteria EAL 4+** in terms of security evaluation level
Products to be delivered without known vulnerability	
Based on the risk and where applicable	
1. Security by default	SECORA™ Connect X comes shipped with a secured configuration by default, including all keys for tokenization, transport security and LCM
2. Protection from unauthorized access	Access is controlled via pre-installed GP Card Content Management Key. Applets come with own keysets.
3. Confidentiality and integrity of data, commands and programs	
4. Minimization of data	
5. Availability of essential functions	
6. Minimize own negative impact on other devices	
7. Limit attack surfaces	Chip access is limited by minimal interfaces I2C and NFC. Communication is OS intern shielded by a secured transaction buffer. No Debug interfaces. No undocumented commands.
8. Reduce impact of an incident	Most sophisticated smartcard grade wear leveling and anti-tearing measures
9. Record and monitor security relevant events	Payment Applet implements Pin Counter and Transaction Counter
10. Enable adequate security updates	SECORA™ Connect X - CC certified in field OS Loader allowing for Applet and data preservation

16 Example of how Infineon can support with CRA compliance: SECORA™ Connect X

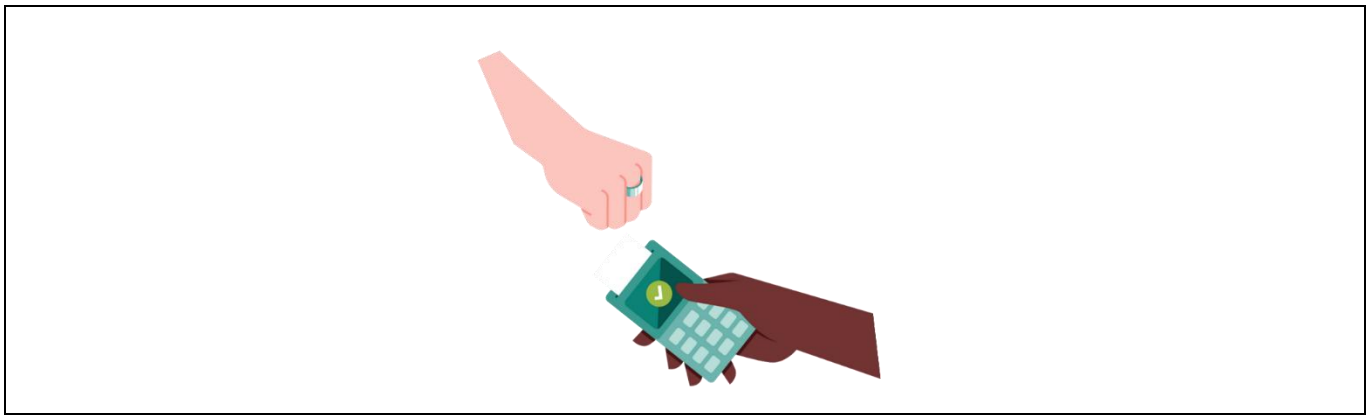


Figure 6 Application example for Payment with Smart Ring embedding SECORA™ Connect X

Based on the threat modelling and asset listing above, the chosen Secure Element is SECORA™ Connect X.

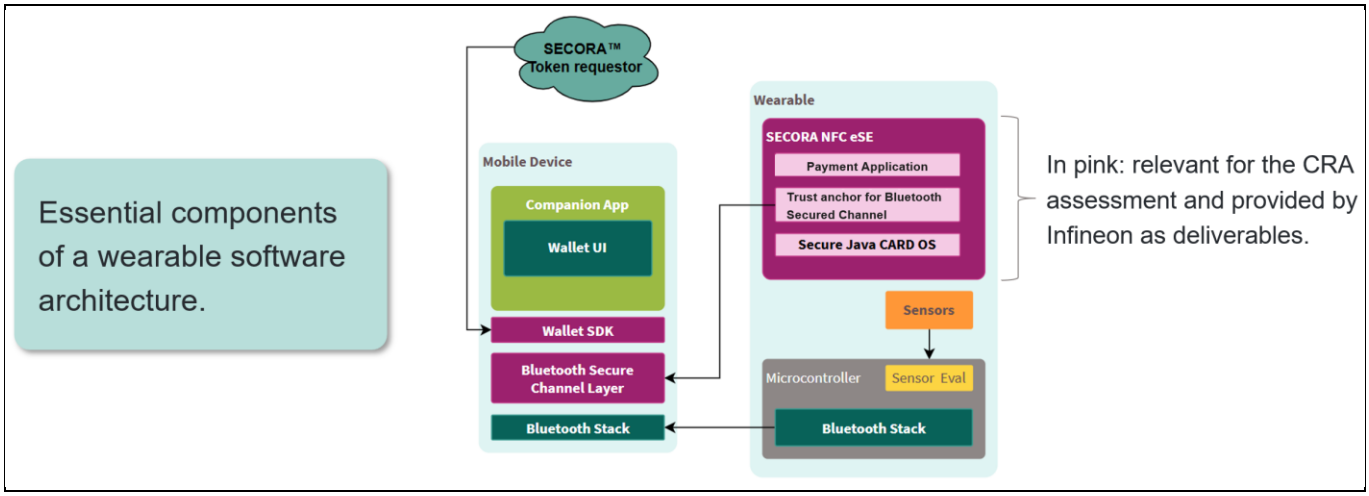


Figure 7 Essential components of wearable software architecture

Going forward, Infineon plans to provide a complete CRA-ready assessment package for our latest ring reference design, including:

- cybersecurity risk assessment (threats, vulnerabilities, mitigations, residual risk),
- required supporting evidence and technical documentation needed for CRA conformity activities.

This package intended for need to be reviewed and signed off by the OEM, significantly reducing effort and time-to-market for ring manufacturers and simplifying CRA compliance for our customers.

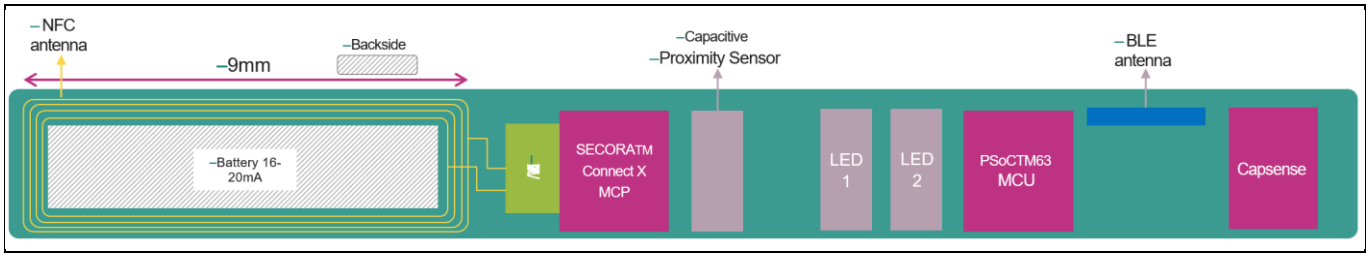


Figure 8 Example for CRA-ready assessment package of smart ring

17 Infineon Edge Systems portfolio broadly supports CRA security regulations

Note: Product categorizations shown below represent Infineon's current technical interpretation and are provided for informational purposes only. Final CRA classification depends on the specific product implementation and applicable regulatory guidance.

Table 6 Mapping of Infineon´s embedded products to the CRA categories

	Product Mapping			
CRA categories	**Default "Unclassified"**	**Important "Class I"[2]**	**Important "Class II"**	**Critical Products**
Class Specification	These are the products which have a lower risk profile compared to other categories.	These are the products that present a higher cybersecurity risk (in terms of it's 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)[3] & 3rd party assessment** Manufacturers shall use hEN if self-assessment or 3rd party assessment to demonstrate that products comply	**Harmonized Standard (hEN) & 3rd party assessment** Manufacturers shall use 3rd party assessment to demonstrate that products comply with an EU legislation (e.g.	**EUCC[4] -** European Cybersecurity Certification A scheme ENISA is developing on behalf of the European Commission to create a framework to certify products

[2] The list of products that are intended to fall into Important Class I can be found in Annex III of the CRA.

[3] Preliminary guidance and subject to changes based on development of CRA harmonized standards, CRA implementation Acts, and any EU Commission- or ENISA- issued CRA guidance. For latest updates refer to EU Commission resources on CRA.

[4] *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.*

17 Infineon Edge Systems portfolio broadly supports CRA security regulations

Product Mapping				
CRA categories	**Default "Unclassified"**	**Important "Class I"[2]**	**Important "Class II"**	**Critical Products**
		with an EU legislation (e.g. EN 50766, PSA L2 / L3)).	EN 50766, PSA L2 / L3)).	with digital elements meet the essential requirements of the CRA. **EN50764 [5]-** standard for smart cards and eSE platforms **EMVCo[6]** a global validation process for payment devices that securely process chip and contactless transactions
Infineon Products enabling CRA	**MCU** • PSOC™ 3 • PSOC™4 / BLE • PSOC™ 5 • XMC™ 1000/4000 **Wi-Fi** • CYW43022 • CYW43012 • CYW4373E • CYW5459x • CYW43907/53907 • CYW43439 • CYW89570	**MCU** • PSOC™ 61/62/63 with BLE 20829 • Wi-Fi6 IoT Combo • PSOC™ Edge8x EPC2 • PSOC™ with BLE • PSOC™ Control C3 • Wi-Fi6 Auto Combo • XMC™ 5000/7000	**MCU (Tamper-resistant MCUs** • PSOC™ Edge8x EPC4 • PSOC™ Edg Next Gen Wi-Fi MCU • ACW **Secure Elements (eSE)**[7] • OPTIGA™ Trust M • OPTIGA™ Trust MTR	**Secure Elements (eSE)** [5] • OPTIGA™ TPM (Common Criteria certified) • OPTIGA™ Connect • SECORA™

[5] 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

[6] 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

[7] CRA requirements can be fulfilled with many MCUs and a discrete Secure Element can make the process easier and more efficient.

17 Infineon Edge Systems portfolio broadly supports CRA security regulations

Product Mapping				
CRA categories	**Default “Unclassified”**	**Important “Class I”[2]**	**Important “Class II”**	**Critical Products**
	AIROC™ Automotive wireless • CYW89459 • CYW89373 **BTBLE** • 2070x/89072 • 20719/20721 • 20819/20820/89820 • 20736/20737 • 20835 • 30739	**Wi-Fi** • AIROC™ CYW5551x • AIROC™ CYW5557x • CYW5553x • ACW74xx / ACW64xx **Wi-Fi MCU** • AIROC™ CYW5591x BT • PSW31xx Wi-Fi/BT MCU • PSB3xxx BT MCU **Secure Memory** – SEMPER™ Secure	• OPTIGA™ Trust M – Express • OPTIGA™ Authenticate	

18 References

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements.

[2] EU Cybersecurity Landscape

[3] European Commission: CE marking – Technical documentation and conformity assessment (official guidance).

[4] Standards bodies: CEN/CENELEC – Harmonized European Norms for CRA essential requirements (in development).

Additional information can be found on webpage Infineon EU-CRA internet site

Revision history

Document revision	Date	Description of changes
1.00	2026-06-24	Initial release
1.01	2026-07-14	Editorial changes
1.02	2026-07-24	Editorial changes

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2026-07-24

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2026 Infineon Technologies AG. All Rights Reserved.

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

Z8F80955683

Important Notice

Products which may also include samples and may be comprised of hardware or software or both ("Product(s)") are sold or provided and delivered by Infineon Technologies AG and its affiliates ("Infineon") subject to the terms and conditions of the frame supply contract or other written agreement(s) executed by a customer and Infineon or, in the absence of the foregoing, the applicable Sales Conditions of Infineon. General terms and conditions of a customer or deviations from applicable Sales Conditions of Infineon shall only be binding for Infineon if and to the extent Infineon has given its express written consent.

For the avoidance of doubt, Infineon disclaims all warranties of non-infringement of third-party rights and implied warranties such as warranties of fitness for a specific use/purpose or merchantability.

Infineon shall not be responsible for any information with respect to samples, the application or customer's specific use of any Product or for any examples or typical values given in this document.

The data contained in this document is exclusively intended for technically qualified and skilled customer representatives. It is the responsibility of the customer to evaluate the suitability of the Product for the intended application and the customer's specific use and to verify all relevant technical data contained in this document in the intended application and the customer's specific use. The customer is responsible for properly designing, programming, and testing the functionality and safety of the intended application, as well as complying with any legal requirements related to its use.

Unless otherwise explicitly approved by Infineon, Products may not be used in any application where a failure of the Products or any consequences of the use thereof can reasonably be expected to result in personal injury. However, the foregoing shall not prevent the customer from using any Product in such fields of use that Infineon has explicitly designed and sold it for, provided that the overall responsibility for the application lies with the customer.

Infineon expressly reserves the right to use its content for commercial text and data mining (TDM) according to applicable laws, e.g. Section 44b of the German Copyright Act (UrhG).

If the Product includes security features:

Because no computing device can be absolutely secure, and despite security measures implemented in the Product, Infineon does not guarantee that the Product will be free from intrusion, data theft or loss, or other breaches ("Security Breaches"), and Infineon shall have no liability arising out of any Security Breaches.

If this document includes or references software:

The software is owned by Infineon under the intellectual property laws and treaties of the United States, Germany, and other countries worldwide. All rights reserved. Therefore, you may use the software only as provided in the software license agreement accompanying the software.

If no software license agreement applies, Infineon hereby grants you a personal, non-exclusive, non-transferable license (without the right to sublicense) under its intellectual property rights in the software (a) for software provided in source code form, to modify and reproduce the software solely for use with Infineon hardware products, only internally within your organization, and (b) to distribute the software in binary code form externally to end users, solely for use on Infineon hardware products. Any other use, reproduction, modification, translation, or compilation of the software is prohibited. For further information on the Product, technology, delivery terms and conditions, and prices, please contact your nearest Infineon office or visit https://www.infineon.com