

The global security regulations landscape with focus on Cyber Resilience Act (CRA)

CSS HOI

public

400%

IoT malware attacks reportedly grew in YoY (2022 to 2023) [2]

EUR 5.5 trillion

estimated global annual cost of cybercrime by 2021 [1]

6.56 billion

connected IOT devices projected in EU by 2030 [3]

[1] European Commission: Joint Research Centre, Baldini, G., Barrero, J., Draper, G., Duch-Brown, N. et al., *Cybersecurity, our digital anchor – A European perspective*, Dewar, M(editor), Coisel, I(editor), Chaudron, S(editor), Nai Fovino, I(editor), Kambourakis, G(editor), Barry, G(editor), Mortara, B(editor), Sanchez, J(editor), Nordvik, J(editor), Junklewitz, H(editor) and Kounelis, I(editor), Publications Office, 2020, **https://data.europa.eu/doi/10.2760/352218**

[2] Zscaler ThreatLabz 2023 Enterprise IoT and OT Threat Report: **https://www.zscaler.com/resources/2023-threatlabz-enterprise-iot-ot-threat-report**

[3] Source: https://explodingtopics.com/blog/number-of-iot-devices

Challenges in securing products/ecosystems & potential impact

Compliance to regulations and standards

Regulations such as US cyber trust mark, EU Cybersecurity Act & upcoming CRA; Standards such as ISA 99, IEC 62443, IEC 61850, NSA Suite

Threats

anti-counterfeiting, unauthorized access, data breaches, and compromises to system integrity and reliability

Mitigating futuristic cybersecurity threats

Requirement for the devices to be in the field for 10+ years, advent of Quantum computers



Potential impacts on users

- Safety risk
- Protection of investment
- Production losses

Potential impacts on brands

- Reputation damage
- Financial loss
- Legal claims
- Market access

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Global IoT Security Regulations landscape 5

2 What is EU CRA: scope, timelines, categories, standards? 10

3 A Practical Guide to prepare for EU CRA 15

4 CRA standardization requirements 19

5 Infineon Solutions enabling EU CRA Compliance 23

6 Key takeaways 31

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 **Global IoT Security Regulations landscape** **5**

2 What is EU CRA: scope, timelines, categories, standards? 10

3 A Practical Guide to prepare for EU CRA 15

4 CRA standardization requirements 19

5 Infineon Solutions enabling EU CRA Compliance 23

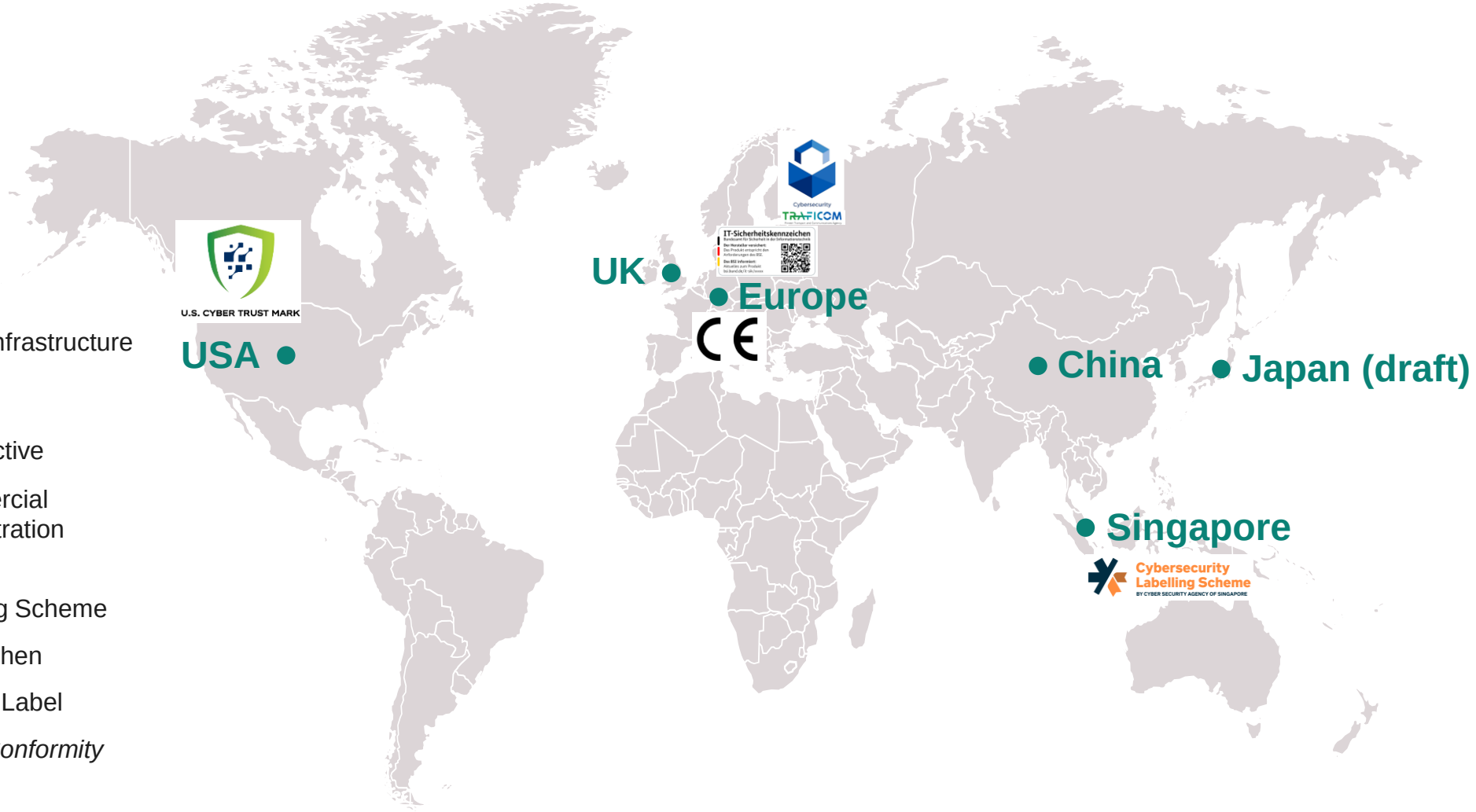
6 Key takeaways 31

Copyright © Infineon Technologies AG 2026. All rights reserved.

Connected devices (IoT) security regulations around the world

USA	U.S. Cyber Trust Mark
UK	Product Security and Telecommunications Infrastructure
European Union	Cyber Security Act Cyber Resilience Act Radio Equipment Directive
China	Office of State Commercial Cryptography Administration (OSCCA) Certification
Singapore	Cybersecurity Labelling Scheme
Germany	IT Sicherheitskennzeichen
Finland	The IoT Cybersecurity Label
Japan	*IoT Product Security Conformity Assessment Scheme**

**in draft proposal state*



Copyright © Infineon Technologies AG 2026. All rights reserved.

Regulation trends – regulation drives need for HW security
EU Regulation, addressing IT, IoT, Safety & Cybersecurity

					In the near future			
IoT vertical	**NIS**	**GDPR**	**CSA**	**RED**	**CRA**	**AI**	**ESPR**	**Others**
Automotive		✓			✓*	✓	✓	Tachograph
Finance	✓	✓		✓	✓	✓	✓	PSD-1/-2, AML-6
Consumer healthcare & lifestyle	✓	✓		✓	✓	✓	✓	MDR-1/-2
5G/6G network	✓	✓	✓	✓	✓	✓		
Industry	✓	✓		✓	✓	✓	✓	
Smart Home/Building		✓		✓	✓	✓	✓	
Cloud services	✓	✓	✓			✓		

AI	**A**rtificial **I**ntelligence Act
AML	**A**nti **M**oney **L**aundering
CSA	**C**yber**s**ecurity **A**ct
CRA	**C**yber **R**esilience **A**ct
ESPR	**E**co-design for **S**ustainable **P**roduct **R**egulation

GDPR	**G**eneral **D**ata **P**rotection **R**egulation
NIS	**N**etwork **I**nformation **S**ecurity **D**irective
MDR	**M**edical **P**roduct **R**egulation
PSD	**P**ayment **S**ervice **D**irective
RED	**R**adio **E**quipment **D**irective

*Vehicle categories M, N, O are explicitly exempt from certain CRA requirements, but vehicle categories L and T are NOT yet exempt.

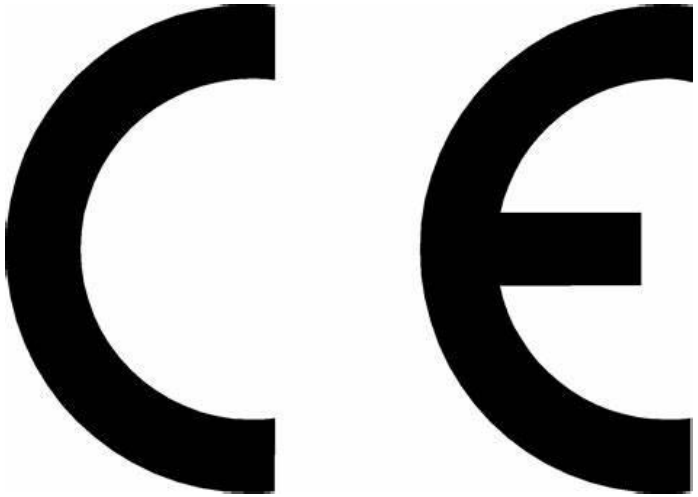
Copyright © Infineon Technologies AG 2026. All rights reserved.

Overview of main IoT Security regulations worldwide

EU Cybersecurity Act	EU Cyber Resilience Act	EU Radio Equipment Directive delegated articles for security and privacy	Singapore Cybersecurity Labelling Scheme	UK Product Security and Telecommunica-tions Infrastructure	US Cyber Trust Mark
– Sets requirements for products, services & processes with focus on security levels: "substantial" and "high" – Is voluntary; redefines ENISA's role and establishes EU cybersecurity certification schemes incl. cloud security and 5G	– Sets requirements for products & components with digital elements sold in EU, 11 December 2027 – Mandatory CE label; has four categories based on risk: default (90% of products), Class I, Class II and Critical *Note: standardization requests and delegated acts are expected from EU Commission that could change the target dates and current definitions in the regulation	– Sets limited requirements for wireless devices connected directly or indirectly to the internet, 1 August 2025 – Mandatory CE label; harmonized RED standard EN 18031-* reuses parts of ETSI EN 303 645	– National label for consumer IoT security based on ETSI EN 303 645 – Co-recognized by Finland, Germany and US IOT security labelling schemes	– Sets 4 requirements for IoT products to be sold in UK, effective since 30 April 2024 – National law for consumer IoT security based on ETSI EN 303 645	– Optional national label for consumer IoT cybersecurity. Is operational since Fall 2024; Launched in CES 2025

Copyright © Infineon Technologies AG 2026. All rights reserved.

EU Cyber resilience act – Declaration of conformity



EU Declaration of conformity
Each CE marked product needs to have an EU declaration of conformity

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Global IoT Security Regulations landscape 5

2 **What is EU CRA: scope, timelines, categories, standards? 10**

3 A Practical Guide to prepare for EU CRA 15

4 CRA standardization requirements 19

5 Infineon Solutions enabling EU CRA Compliance 23

6 Key takeaways 31

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	**Automotive**	**Marine Equipment**	**Civil Aviation**	**IT, Cloud, SaaS**
EU MDR-2	UNECE R155		certified	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 timelines and transition milestones

Nov/2024



The CRA Regulation
is published.

Sep/2026
+21 months



Obligations begin
on incidence reporting.

Dec/2027
+36 months



Full Compliance
is enforced on products and process.

*Note: standardization requests, delegated acts expected from EU Commission that could change the target dates.

CRA Product Categories and their Compliance Requirements

Default "Class 0"	Important products "Class I"	Important products "Class II"	Critical products
'catch-all category'	Examples	Examples	Examples
All products with digital elements (HW, SW, including remote data processing) **not listed in** important, critical, or exempted product categories	Smart home devices with security functions, routers, modems, connected toys, personal wearables, ID, biometric, access control,…	Hypervisors and container runtime environments, VPN, Firewalls, Tamper-resistant Microcontrollers, and Microprocessors, …	smartcards, secure elements and similar devices, smart meter gateways, advanced security systems, …

Self assessment

Self Assessment based on EU harmonized standard*

3rd Party Assessment: Internal Production Control, Full QA

EU cybersecurity certification**

* EU harmonized standards development are commissioned by EU Commission; in absence, 3rd Party assessment by Notified bodies is required
** Direct use of EU cybersecurity certification as a CRA demonstration conformity can be allowed through a EU Delegated Act.

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.

Table of contents

1 Global IoT Security Regulations landscape 5

2 What is EU CRA: scope, timelines, categories, standards? 10

3 **A Practical Guide to prepare for EU CRA** **15**

4 CRA standardization requirements 19

5 Infineon Solutions enabling EU CRA Compliance 23

6 Key takeaways 31

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

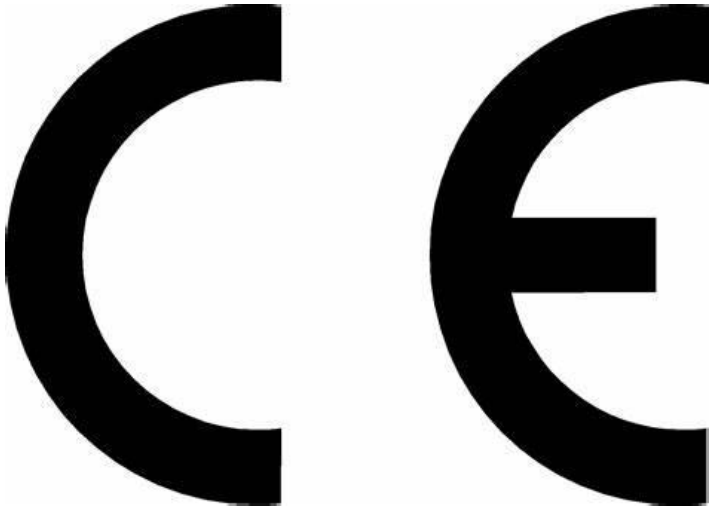
- Security-by-design
- Vulnerability management
- CE documentation, security tests

Copyright © Infineon Technologies AG 2026. All rights reserved.

Evidence and documentation plan – an example

- Risk assessment
- Security test 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 2026. All rights reserved.

Table of contents

1 Global IoT Security Regulations landscape 5

2 What is EU CRA: scope, timelines, categories, standards? 10

3 A Practical Guide to prepare for EU CRA 15

4 **CRA standardization requirements** **19**

5 Infineon Solutions enabling EU CRA Compliance 23

6 Key takeaways 31

Copyright © Infineon Technologies AG 2026. All rights reserved.

CRA harmonized standards development landscape

Note: Available draft versions for public review are linked below

Vertical standards for the product types in Class I, Class II and Critical [1]

TC CYBER-EUSR

ETSI has opened various standards for public consultation for wearables, Smart home, firewalls, browsers, hypervisors and virtual containers, OS, VPNs, PKIs, boot managers etc.

The latest versions you can find under this link.

TC 47X

semiconductors in Class I, Class II and Critical

For details see next slide.

CENELEC TC65X

SIEM, network management for IACS

TC 224

- Applications for smart cards and secure elements, identity management systems

(The latest version you can find under this link)

- Hardware with security boxes

Horizontal standards as common baseline for all vertical standards

JTC 13

Cybersecurity requirements for products with digital elements

- Principles for cyber resilience [1] (The latest version you can find under this link)
- Vulnerability handling [1] (The latest version you can find under this link)
- Generic security requirements [2]

1 – Expected date of publication of these standards – 30 Oct 2026.
2 – Expected date of publication of these standards – 30 Oct 2027.

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 discussion

- The mature drafts of EN 50765, EN 50766 and EN50764 have entered public enquiry phase.
- 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.

Table of contents

1 Global IoT Security Regulations landscape 5

2 What is EU CRA: scope, timelines, categories, standards? 10

3 A Practical Guide to prepare for EU CRA 15

4 CRA standardization requirements 19

5 **Infineon Solutions enabling EU CRA Compliance** **23**

6 Key takeaways 31

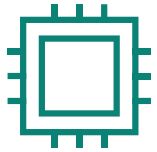
Copyright © Infineon Technologies AG 2026. All rights reserved.

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...

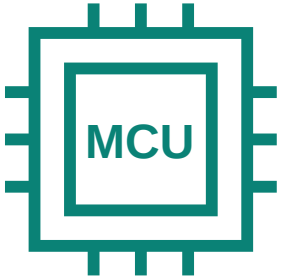
...and how Infineon products help fulfil them

CRA obligation	Engineering requirement	Infineon solution/s
No Unauthorized Access	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	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

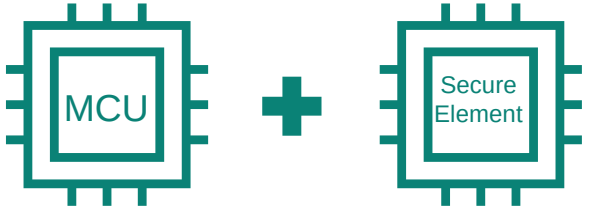
MCU/ MPU



?

When does it need a dedicated

HW-security-anchor?



Choose 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
- ✓ Device identity anchored in hardware root-of-trust. Support for secured communication (TLS).
- ✓ TCG 2.0-compliant, measured boot with PCRs; remote attestation.
- ✓ Strong key storage and crypto operations offload.
- ✓ Anchor SBOM integrity via sealed hash.

OPTIGA™ Trust M "IoT security made easy"

- ✓ Secure Element (SE) with ECC, symmetric crypto, secured key storage.
- ✓ 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.

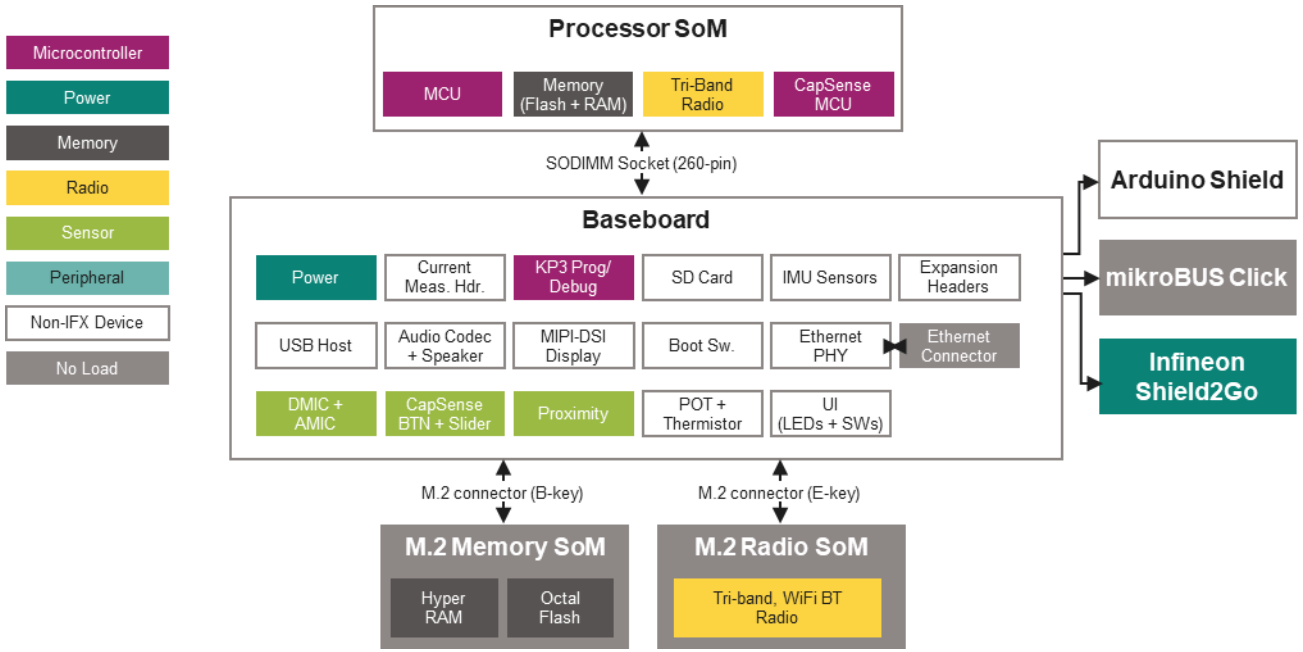
... to enable EU CRA Security outcomes

- 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.

Reference Architecture – PSOC™ Edge E84 Evaluation Kit





Kit features

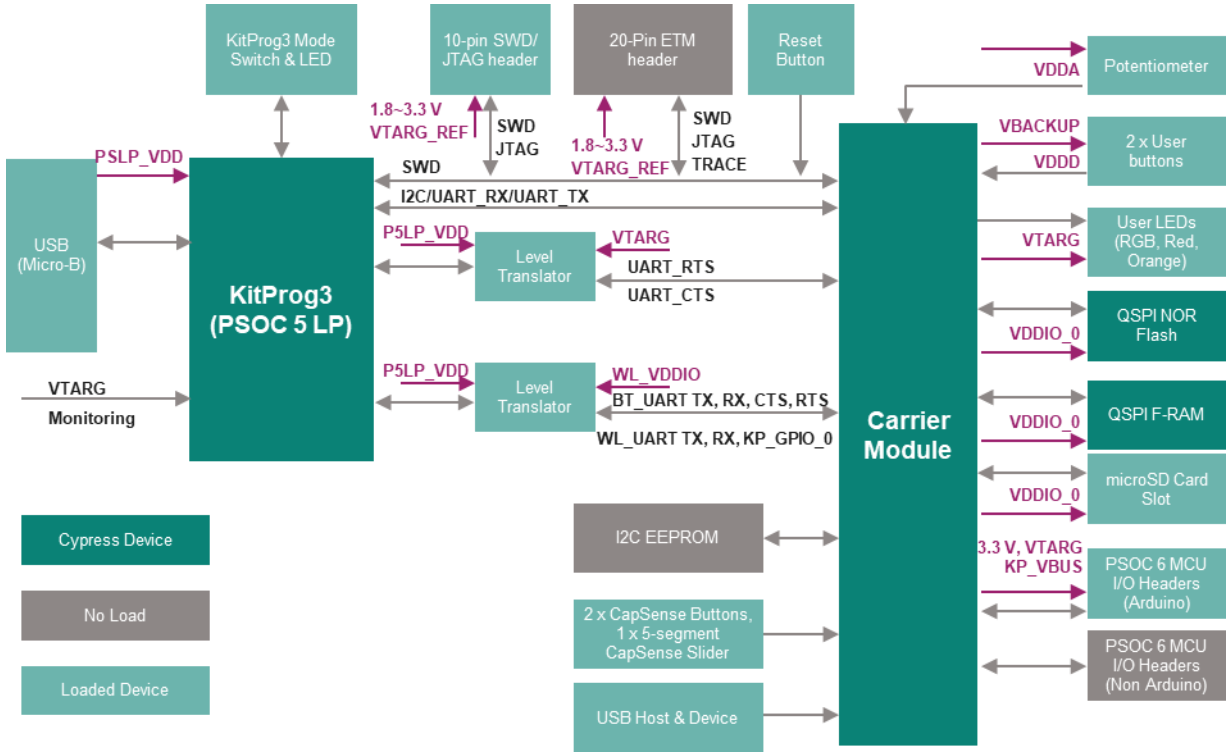
- **build EU CRA default, important class device references**
- PSOC™ 4000T as CAPSENSE™ coprocessor
- Supported by ModusToolbox™ and DEEPCRAFT™ AI Suite
- Many code examples for security
- Onboard AIROC™ Wi-Fi & Bluetooth™ combo
- Analog and PDM microphones
- 6-axis accelerometer, gyroscope IMU, 3-axis 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.

Reference Architecture – PSOC™ 6 WiFi-BT Pioneer Kit





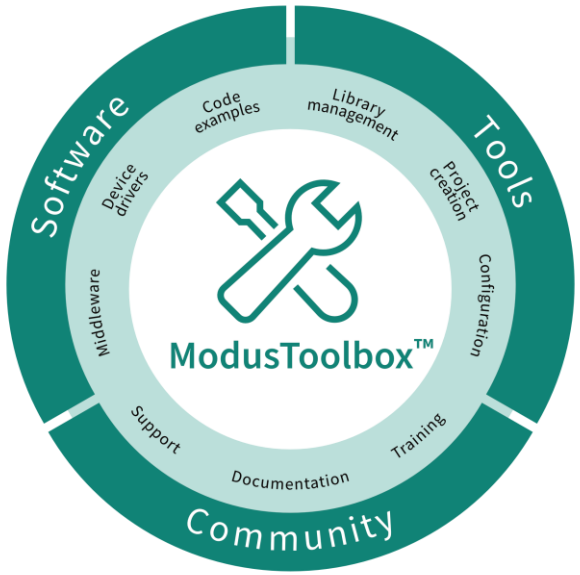
Kit features

- **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.

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.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Table of contents

1 Global IoT Security Regulations landscape 5

2 What is EU CRA: scope, timelines, categories, standards? 10

3 A Practical Guide to prepare for EU CRA 15

4 CRA standardization requirements 19

5 Infineon Solutions enabling EU CRA Compliance 23

6 **Key takeaways** **31**

Copyright © Infineon Technologies AG 2026. All rights reserved.

Act now!



Resources for you:

- Order rapid sampling and evaluation kits.
- Request dedicated technical meetings to architect security in your product
- Ask for dedicated CRA workshops/trainings for your engineering teams.
- Get access to application notes, code examples for PSOC™, OPTIGA™, and start building CRA security outcomes into your product



Assets to request:

- **See which part is right for you** using Infineon embedded application mapping across (indicative) CRA category**
- **Get a development kit:**
  - PSOC™ 6 WiFi-BT Pioneer Kit
  - PSOC™ Edge E84 Evaluation Kit
- **Download ModusToolbox™ software** – Infineon's tool to develop CRA applications

**Disclaimer: this is preliminary guidance and subject to changes based on CRA harmonized standards (in-development), CRA (future) implementation Acts, and any EU Commission- or ENISA- issued CRA guidance. For accuracy kindly refer to EU Commission resources on CRA.

Copyright © Infineon Technologies AG 2026. All rights reserved.

Most of the CRA security requirements are still in development but will have a profound effect globally once they come into force

- Integrate "Security by Design" and EU CRA Security outcomes into your product
- Establish robust Vulnerability Management and CE labelling processes for EU CRA compliance
- Leverage Infineon Security Solutions to add EU CRA security outcomes to your IoT devices



Copyright © Infineon Technologies AG 2026. All rights reserved.

Visit Infineon's CRA webpage for more information and FAQs on this topic

