MINDSHARE26

CYBERSECURITY LEADERSHIP FORUM

NXP

EU Cyber Resilience Act – what does it mean for you?

Mario Stoltz, Carlos Serratos
NXP Semiconductors

11.06.2026 | WISSENSCHAFTSPARK | GELSENKIRCHEN

EVIDEN

DISCLAIMER

- Statements in this presentation do not constitute legal advice. They represent the views of the presenter and/or the best-effort and bona fide interpretations of NXP for our own products
- The CRA applies to any entity bringing products to market in the EU. Every such entity is responsible to follow the CRA and related standards and regulations

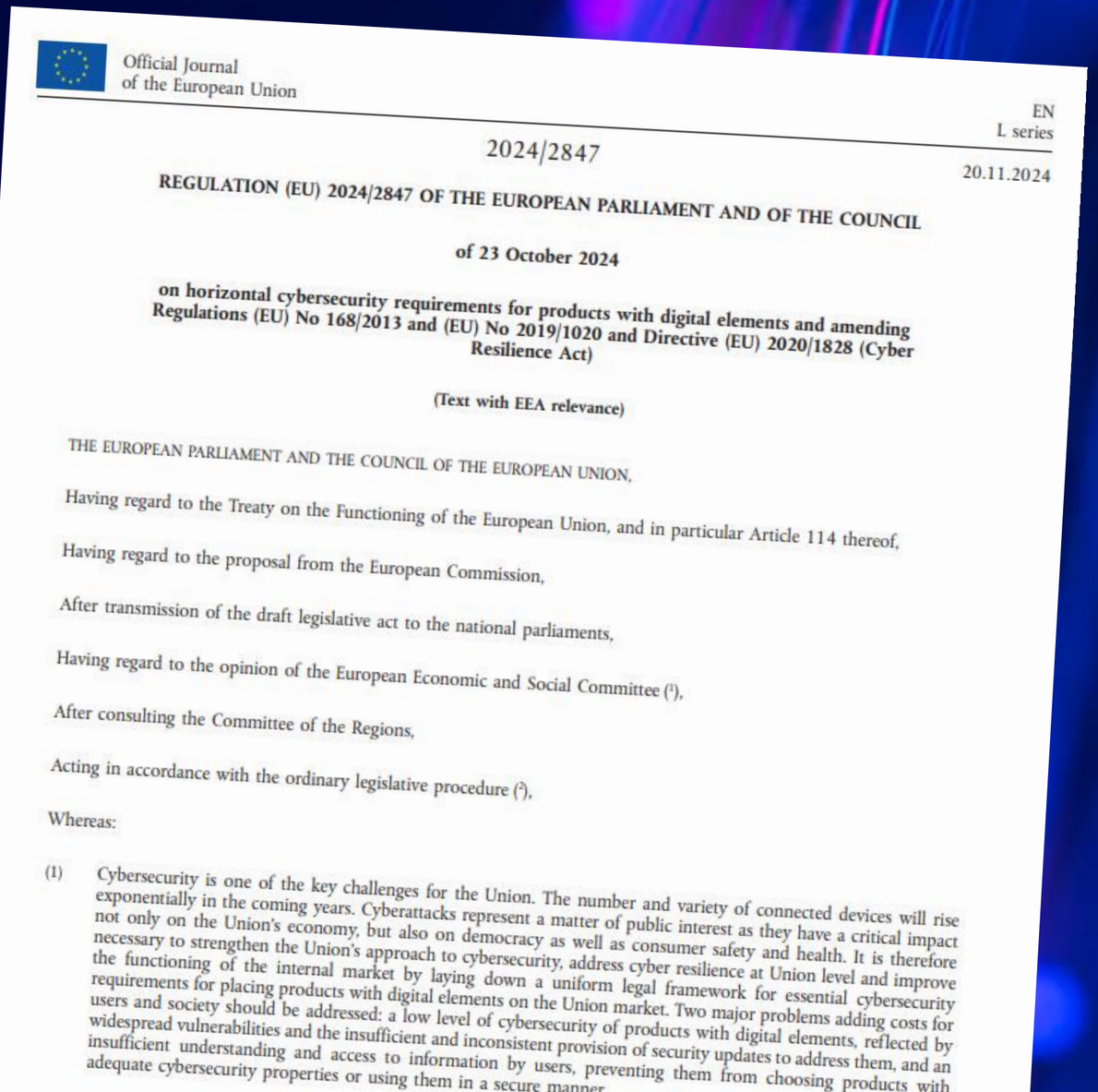
MINDSHARE26

EVIDEN

NXP

AGENDA

1. **Overview**
2. New requirements
3. Who (what) is affected how?
4. Resources
5. Summary



Official Journal of the European Union

EN
L series

2024/2847

20.11.2024

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 and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure ([2]),

Whereas:

(1) Cybersecurity is one of the key challenges for the Union. The number and variety of connected devices will rise exponentially in the coming years. Cyberattacks represent a matter of public interest as they have a critical impact not only on the Union's economy, but also on democracy as well as consumer safety and health. It is therefore necessary to strengthen the Union's approach to cybersecurity, address cyber resilience at Union level and improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. Two major problems adding costs for users and society should be addressed: a low level of cybersecurity of products with digital elements, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner.

Overview / the bare facts

- regulation (EU) 2024/2847 was published in December 2024
- Specific requirements come into force between September 2026 and December 2027
- Regulation text apparently mostly written with “finished products” in mind (not e.g. “components”), both HW and SW. However, components are *clearly in scope*
- Applicable to “products with digital elements” that are placed on the market in the EU, regardless of their origin. In practice, products that “store, communicate or otherwise process data at rest or in transit”
- Mandatory cybersecurity requirements for affected products

Requirements (high level)

- Cybersecurity by design and by default*
- Essential cybersecurity requirements (ECRs) and vulnerability handling requirements, including reporting obligations
- Conformity assessment and compliance (depending on product category)
- Interplay between conformity assessment procedure and further cybersecurity legislation
- Fines for manufacturers, importers, distributors up to 15M€ or 2.5% of annual global revenue

*) e.g.: no more weak default passwords

EVIDEN

NXP

Essential Cybersecurity Requirements

- protect data confidentiality & integrity
- enable automated updates of embedded software (assuming the product can communicate, process data and has embedded SW)
- have capabilities for authentication
- perform activity logging
- have capabilities for secure erase and backup

Details for all these requirements will be provided in harmonized standards

Who / what is affected how?

- **Manufacturers** – full CRA validity
- "**MSME**s" (microenterprises, small and medium-sized enterprises) – also full CRA validity, but *support, simplified technical documentation, alleviated administrative compliance burden*
- **Open source developers** – not in scope, unless code provision is monetized. Contribution to OSS/free SW not in scope. However, continue checking!

What must be done in detail?

Security requirements

- Security by design & by default
- No known vulnerabilities
- Provide security updates
- Access control (to PwDE)
- Protect confidentiality & integrity
- Minimize data
- Keep basic functionality available despite of incident
- Minimize negative impact around PwDE
- Limit attack surface
- Actively mitigate incidents
- Status recording & monitoring
- Allow user to delete data & settings

Vulnerability handling requirements

- Identify and document components and vulnerabilities
- Address vulnerabilities
- Perform regular security testing
- Publish fixed vulnerabilities
- Implement and practice vulnerability disclosure policy
- Support 3rd party reporting
- Dissemination of updates
- Ensure secure distribution of updates

The unmanageable monster in the CRA

Security requirements

- Security by design & by default
- No known vulnerabilities
- Provide security updates
- Access control (to PwDE)
- Protect confidentiality & integrity
- Minimize data
- Keep basic functionality available despite of incident
- Minimize negative impact around PwDE
- Limit attack surface

Just *slightly* off topic

EVIDEN

NXP

How to pronounce PwDE??

Option	Mnemonic image	DE	EN

Just *slightly* off topic

EVIDEN

NXP

Product categories

Category	Defined in…	Example
Critical	Annex IV of the CRA	This is the full list: **1. Hardware devices with security boxes** 2. Smart meter gateways within smart metering systems […] and other devices for advanced security purposes, including for secure cryptoprocessing **3. Smartcards or similar devices, including secure elements**
Important (class 2)	Annex III of the CRA	This is the full list: 1. Hypervisors and container runtime systems 2. Firewalls, intrusion detection and prevention systems 3. Tamper-resistant microprocessors 4. Tamper-resistant microcontrollers
Important (class 1)	Annex III of the CRA	19 items, among them: **Identity**/network **management systems** Microprocessors/controllers with security-related functionalities Smart home products with security functionalities Personal wearables for health monitoring
Default	Legislative intention: 90% of products should fall into this category	Hard drives Smart speakers Robot vacuum Games and toys
(Not regulated)		Products not intended to be placed on the EU market or without digital elements, including open-source SW not intended for commercial activity

NOTE: "lower" category does not mean lower security requirement. These are a result of your risk assessment. Different category means different mechanism to demonstrate conformance

Conformance mechanism per category

Category	Default category	Important Product "Class I"	Important Product "Class II"	Critical Products
Minimum conformance mechanism	**Self-assessment**	**Harmonized standards** (ensuring CRA principles are met)	3rd Party product assessment (product and/or process)	**Common Criteria certification by default**

Determine your product's criticality early and plan for the required conformance mechanism

This step drives design choices and compliance effort. Anticipate early to avoid delays

not public

Technical Documentation

Risk assessment * architecture * test results * SBOM * update mechanisms * conformance rationale

not public

Declaration of conformity / CE mark

public

Post-market

monitor * fix * report* maintain

not public

EVIDEN

NXP

Harmonized standards

- For specific application areas and / or product types, there will be European standards that specify which cybersecurity properties, cryptographic protocols, key lengths and which security assessment method is appropriate under the CRA
- Development of harmonized standards has been assigned to CEN/CENELEC and ETSI
- Voluntary use by manufacturers, adherence provides presumption of conformity

MINDSHARE26

EVIDEN

NXP

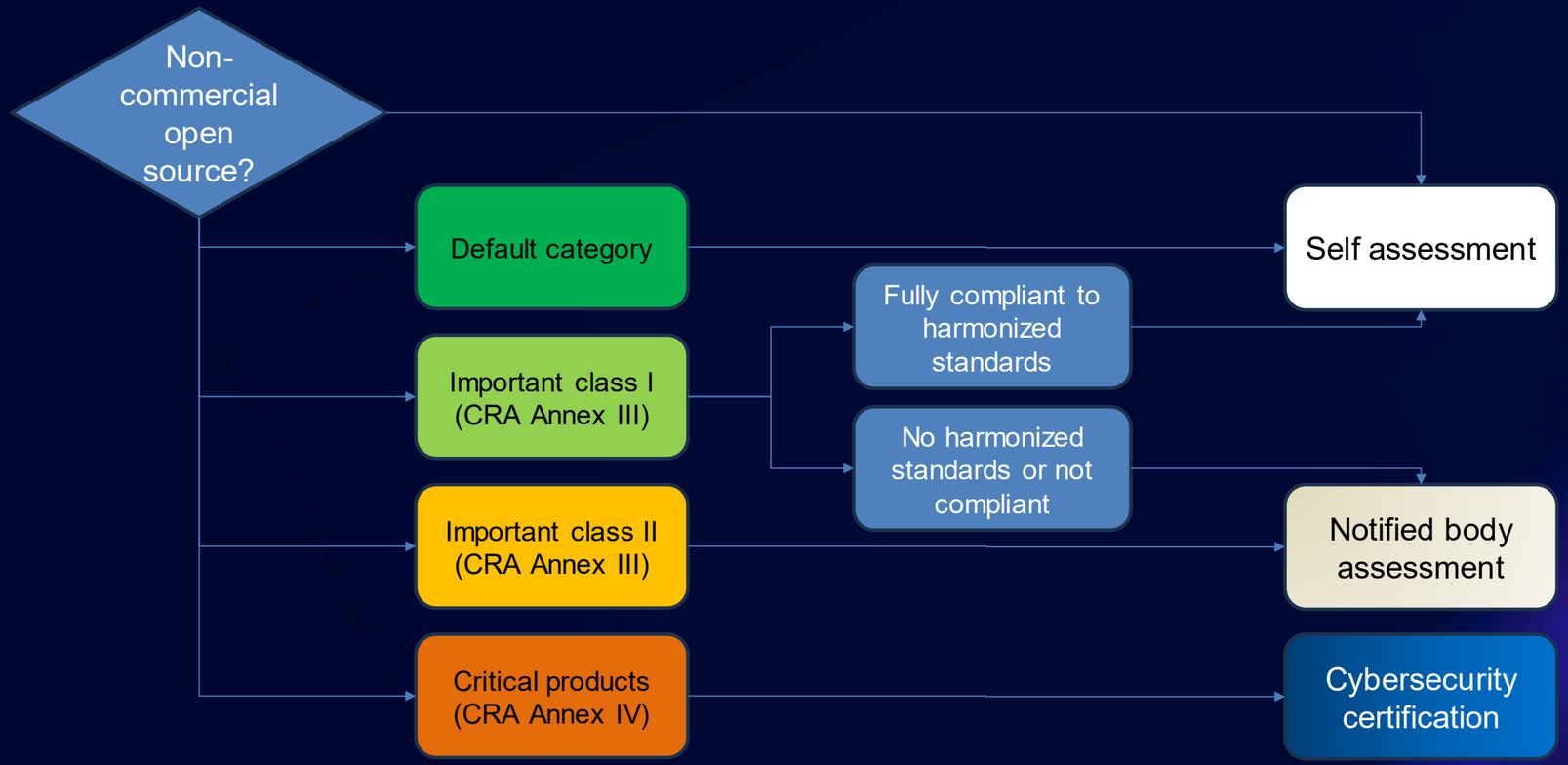
Harmonized standards

M/606	Technical Committee(s)		In collaboration with	Work Item	M/606 - Planning for standard development			
Topics M606 - Annex I	TC ref.	TC title			Standard reference	Standard title	Last realized stage	Deadline for adoption
Line 1: European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks								
1	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013089	*EN xxxxxx (Will be be defined after the activation of the Work Item)*	Cybersecurity requirements for products with digital elements — Principles for cyber resilience	10.99 - NWI - New Work Item adopted	2026/08/30
Lines 2-14 - European standard(s) CRA essential requirements								
2 to 14	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013091	*EN xxxxxx (Will be be defined after the activation of the Work Item)*	Cybersecurity requirements for products with digital elements – Generic Security Requirements	10.99 - NWI - New Work Item adopted	2027/10/30
Line 15: European standard(s) on vulnerability handling for products with digital elements								
15	CEN-CLC/JTC 13 WG 9	Cybersecurity and Data Protection	N/A	JT013090	*EN xxxxxx (Will be be defined after the activation of the Work Item)*	Cybersecurity requirements for products with digital elements – Vulnerability Handling	10.99 - NWI - New Work Item adopted	2026/08/30
Line 16: European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers								
16	CEN/TC 224 WG 17	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	CEN/TC 224 WG 17 (including expertise from WG 18,19 and 20) TC ESI	002242XX	*EN xxxxxx (Will be be defined after the activation of the Work Item)*	Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers : criteria to fulfill with the essential requirements from regulation 2024/2487 (CRA)	TC decision taken	2026/10/30
Line 17: European standard(s) on essential cybersecurity requirements for standalone and embedded browsers								
17a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(Will be be defined after the adoption of the Work Item)*	*EN 304 617-1*	European standard(s) on essential cybersecurity requirements for embedded browsers	PWI - Proposed Work Item created	2026/10/30
17b	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(Will be be defined after the adoption of the Work Item)*	*EN 304 617-2*	European standard(s) on essential cybersecurity requirements for standalone browsers	PWI - Proposed Work Item created	2026/10/30
Line 18: European standard(s) on essential cybersecurity requirements for password managers								
18	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(Will be be defined after the adoption of the Work Item)*	*EN 304 618*	European standard(s) on essential cybersecurity requirements for password managers	PWI - Proposed Work Item created	2026/10/30
Line 19: European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software								
19	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9	*(Will be be defined after the adoption of the Work Item)*	*EN 304 619*	European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software	PWI - Proposed Work Item created	2026/10/30
Line 20: European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)								
20a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9 CLC/TC 65X WG3 mode 2	*(Will be be defined after the adoption of the Work Item)*	*EN 304 620*	European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)	PWI - Proposed Work Item created	2026/10/30
20b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	ETSI TC Cyber EUSR Mode 2	81652	*EN 62443-5-XX (Will be be defined after the activation of the Work Item)*	Security Profile for products with digital elements with the function of virtual private network (VPN)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 21: European standard(s) on essential cybersecurity requirements for network management systems								
21a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	CEN-CLC/JTC 13 WG 9 CLC/TC 65X WG3 mode 2	*(Will be be defined after the adoption of the Work Item)*	*EN 304 621*	European standard(s) on essential cybersecurity requirements for network management systems	PWI - Proposed Work Item created	2026/10/30
21b	CLC/TC 65X WG 3	Industrial-process measurement, control and	ETSI TC Cyber EUSR Mode 2	81650	*EN 62443-5-XX (Will be be defined after the activation of the Work Item)*	Security Profile for network management systems (based on IEC 62443)	00.60 - PWI - Preliminary Work Item created	2026/10/30

EVIDEN

NXP

Certify or no certify? Find out for yourself you must!



…but software?

- When does it count as “placed on EU market”?
  - Conservative assumption: everything published by an EU company except if…
  - …only provided to non-EU customers
  - …license prohibits use in the EU
- When does it count as “product” under the CRA?
  - Conservative assumption: any SW **except** if…
  - …a fragment/unfinished, part of documentation/training material
  - …free/open-source SW published in a public research project
  - …part of a cloud service / SaaS model (Note: might still be in scope if service used by another product)

Notable items for software

- Annex I part II explicitly requires a SW BOM
- Provide security updates, separately from functionality updates where feasible
- Share and disclose information about fixed vulnerabilities after an update; delays allowed for risk balancing reasons
- Provide instructions for commissioning *and de-commissioning* and removal of user data

OK so *what* do I do now?

#1 risk assessment:

- Identify assets that need protection
- Understand applicable threats based on real-world use conditions (likelihood, impact)
- Determine suitable technical and procedural mitigations and *how these will address the CRA essential cybersecurity requirements*
- *identify and establish the correct product classification under the CRA*

…then take it from there (e.g. follow harmonized standard)

#2 adopt security by design

#3 provide credible evidence of compliance (ECRs, documentation, conformity assessment)

#4 maintain conformity across lifecycle (vulnerability management, SW+doc updates)

EVIDEN

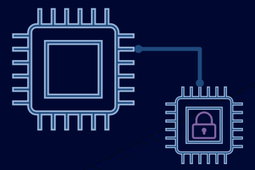
NXP

How does someone like NXP help?

EdgeLock Secure Enclave

Dedicated security unit integrated in NXP MCU/MPU

- ✓ Enhanced isolation for protection of critical security functions required by regulations
- ✓ Advanced capabilities for device monitoring and availability protection
- ✓ Protection of sensitive data and credentials
- ✓ Available on latest NXP MCU/MPUs



EdgeLock SE05x/A30

Secure elements and secure authenticators

- ✓ Secure vault for credentials with protection against SW and advanced HW attacks
- ✓ Certified Common Criteria EAL6+, FIPS 140-3
- ✓ Optional personalization with custom credentials injected at NXP manufacturing
- ✓ Can be plugged to any type of ASIC or processor

EdgeLock 2GO

NXP cloud services for credential management

- ✓ Easy deployment of root of Trust credentials on devices
- ✓ Management of credentials over-the-air and throughout device lifecycle
- ✓ Native integration on EdgeLock Secure Enclave, Secure Elements and Secure Authenticators
- ✓ Supports CRA post-market obligations (updates, vulnerability handling, revocation)

Simplify CRA compliance and strengthen resilience with integrated hardware, secure components, and lifecycle services.

Resources / further reading

- EU landing page for CRA with summary, Q&A, guidance, national ref's
- CRA source text and implementing regulation 2025/2392 on eur-lex
- CEN/CENELEC and ETSI work programme for CRA related standards, especially *EN 304* and *EN 62443* series
- ETSI TC CYBER overview
- M.-J. Saarinen: *CRA and cryptography – the story thus far* (paper, PPT)
- NXP landing page on CRA, including whitepapers, presentations, application notes
- Infineon landing page, STM Q&A or deep dive
- Agreed cryptographic mechanisms at ENISA

Closing thoughts

- Any security problem has multiple solutions. If a manufacturer uses a weak component, then they will have to introduce more countermeasures on another level. If they use a stronger component, there is less they must do
- The key challenge of CRA is not technology, certification or compliance, but ***culture change***. Every manufacturer must learn to live security by design and active lifecycle management. Company cultures need to change, and how you work with suppliers / development partners.

MINDSHARE26

CYBERSECURITY LEADERSHIP FORUM

NXP

Questions?

Mario Stoltz, NXP Semiconductors
mario.stoltz@nxp.com