It's The Law:
Some Technical Things All Hardware Security Architects Ought to Know About CRA, EUCC

Markku-Juhani O. Saarinen
<markku-juhani.saarinen@tuni.fi>

October 17, 2025 -- FAU, Boca Raton

Tampereen yliopisto
Tampere University

Hello! 👋 I'm **Markku-Juhani Saarinen.**

- Cryptographer for some 30 years (started professionally at SSH Communications Security, Helsinki) in 1997. PhD Royal Holloway, University of London (2009).
- Academia and industry, most recently in industry at PQShield from 2018 to 2024.
- Currently Professor of Practice at Tampere University in Finland.
- Ask me about RISC-V: Cryptography SIG Chair, PQC TG Chair at RISC-V International.
- **Background on this talk**: I wanted to find out about CRA, had to join the committees..

The information in this talk represents my own personal views only.

NOTE – PRELIMINARY INFORMATION, VERY LIKELY TO CHANGE

OUTLINE

1. The Cyber Resilience Act (CRA) and closed standards

2. "Amsterdam Proposal" on how EU may specify crypto requirements

3. ~~Little bit about product categories and EUCC (EU Common Criteria)~~

My mouse? Raincoat? Plush toy?

CRA: Cyber security meets the CE Mark

- Electrical products can not be sold in Europe without a CE mark (there are serious fines.)

- CE requirements are defined in EU directive(s) / regulation(s) and harmonised standards.

- Compliance with **EU Cyber Resilience Act (CRA)** is **required** for a CE mark from December 2027.

The official **“Blue Guide”** on the implementation of EU product rules:

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52016XC0726(02)

Some Euro Standards Lingo (very informally)

Harmonized Standards: *Following harmonized standards in the design and manufacture of your products will ensure your products are in line with corresponding EU rules; this is known as "presumption of conformity."*

Horizontal Standards: *Product-agnostic ("general purpose") and framework-oriented, providing foundational guidance applicable across sectors.*

Examples: *Vulnerability reporting processes, SBOM (Software Bill of Materials.)*

Vertical Standards: *Product-specific, offering targeted requirements for particular categories of digital products.* ***Examples:*** *Browsers, VPNs, Processors*

EC Requested **CRA** Standards from **EU** Std. Orgs

I wanted to study the **CRA** draft security standards (at **CENELEC**, **CEN,** and **ETSI**.)

A **FI** person needs to be appointed into those by three different national standardization committees **SESKO**, **SFS**, and **TRAFICOM** (replace with yours.)

We paid a €600 annual fee and I joined SESKO, who appointed me to TC 47x. SFS put me into their SR 307 for CEN. ETSI worked out after I became a rapporteur.

CEN-CENELEC works a lot like ISO-IEC:

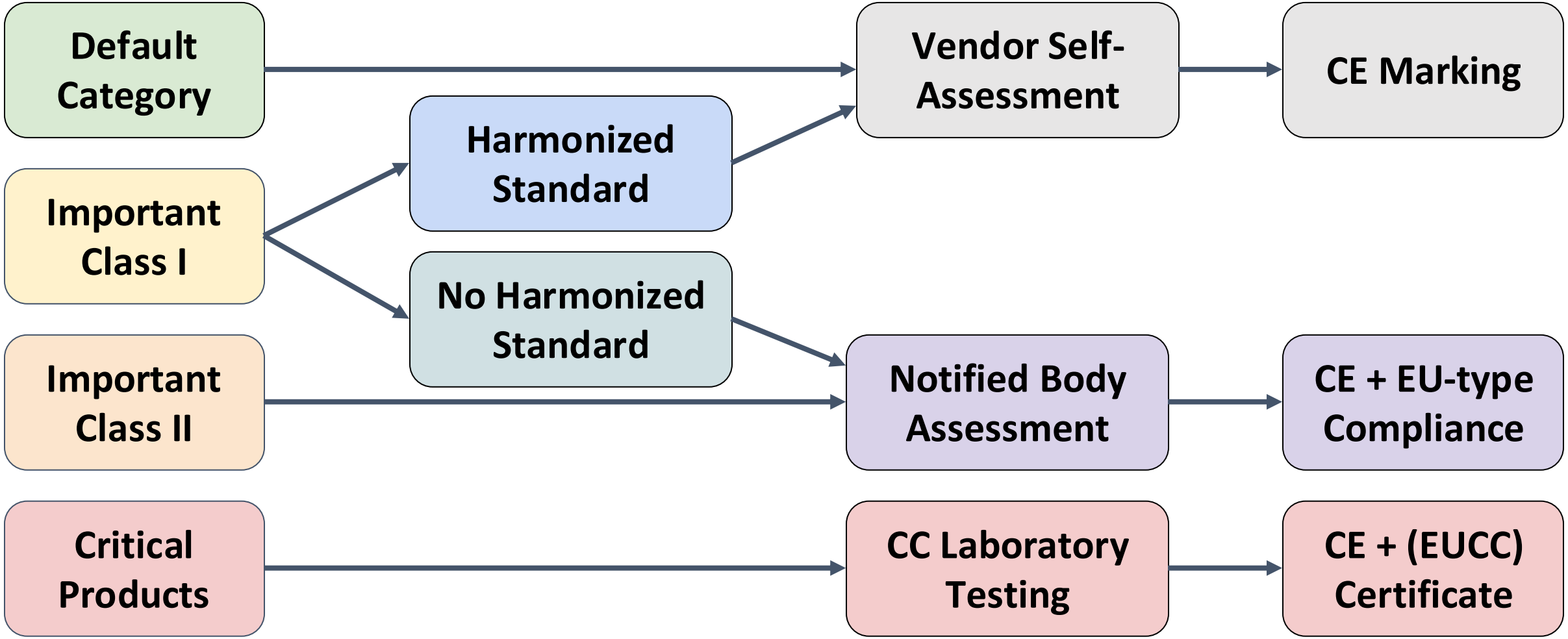
Almost no-one has visibility to the standards before they actually come out.

Only then they can be purchased for €50 .. €300 per document (1 seat!) ≈ *no one does that.*

Security risks from this process (compared to crypto competitions, IETF, ETSI/3GPP):

- **Limited public review leads to low quality.** No drafts, open mailing lists etc. The participation of scientific experts "inside" the processes is challenging (no publications!)
- **Watering down**: Some corporations participate in CRA standardization mainly to minimize the re-engineering effort and cost on their own product lines. Why would they make things harder for themselves? A harmonized standard is a way to influence this.
- **Risk of Backdoors or bad crypto.** The NSA-backdoored "Dual EC" RBG was removed from ISO 18031 in 2014 but suspect Micali-Schnorr RBG remained until the 2025 revision.

CRA Product Categories *(Grossly simplified)*



Default Category (in electrotechnical products)

Most software and hardware product types that are **not** mentioned in Annex III are in the **Default category,** unless:

- The product provides security functions to others.
- The product can disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation.

In the default category, vendor's "internal controls" suffice.

Excluded from CRA (covered by other EU laws): *Medical devices, in vitro diagnostic devices, automotive-related devices, marine equipment, aviation certified devices.*

Each Annex III item will have a vertical standard..

CRA Annex III, Important Class I		
1	(Line 16, CEN)	Identity management systems and privileged access management software and hardware (CEN/TC 224 WG 17)
2	ETSI EN 304 617	Browsers
3	ETSI EN 304 618	Password managers
4	ETSI EN 304 619	Software that searches for, removes, or quarantines malicious software
5	ETSI EN 304 620	Virtual Private Networks (VPNs) (part 1 and 2)
6	ETSI EN 304 621	Network Management systems
7	ETSI EN 304 622	Security information and event management (SIEM) systems
8	ETSI EN 304 623	Boot managers
9	ETSI EN 304 624	Public key infrastructure and digital certificate issuance software
10	ETSI EN 304 625	Physical and virtual network interfaces
11	ETSI EN 304 626	Operating systems
12	ETSI EN 304 627	Routers, modems intended for the connection to the internet, and switches
13+14	**CLC EN 50765**	**Microprocessors and microcontrollers (Self-assessment, 47X WG 1)**
15	**CLC EN 50767**	**ASICs and FPGAs with security-related functionalities (47X WG 4)**
16	ETSI EN 304 631	Smart home general purpose virtual assistants
17	ETSI EN 304 632	Smart home products with security functionalities (locks, cameras, baby monitoring, alarm)
18	ETSI EN 304 633	Internet connected toys
19	ETSI EN 304 634	Personal wearable products to be worn or placed on a human body

.. more: **Important Class II** and **Critical**

CRA Annex III, Important Class II		
1	ETSI EN 304 635	Hypervisors and container runtime systems
2	ETSI EN 304 636	Firewalls, intrusion detection and/or prevention systems
3+4	**CLC EN 50766**	**Microprocessors and microcontrollers (Moderate and high-risk environments, WG 2)**
CRA Annex IV, Critical		
1	(Line 39, CEN)	Hardware Devices with Security Boxes (CEN/TC 224 WG 17)
2	(Line 40, CEN-CLC)	Smart meter gateways within smart metering, secure cryptoprocessing (CEN-CLC/JTC 13 WG 6)
3	**CLC EN 50764**	**Smartcards or similar devices, including secure elements (47X WG 3)**

CEN-CLC/JTC 13 WG 9 has several “essential requirements” horizontal standards:

Risk-based approach, Principles for cyber resilience, Generic Security Requirements, Vulnerability Handling, SBOM (Software Bill of Materials)

-> we may have dependencies on these, but not much visibility to their work.

CLC/TC 65X WG 3 is developing **six** further vertical standards covering CRA requirements, but in the context of **Industrial Automation and Control**.

Meanwhile in America - Much Smaller Scope

To address cyber security in consumer IoT products (only), U.S. Federal Communications Commission (FCC) in 2023 announced a voluntary **“U.S. Cyber Trust Mark”** program.

The program is inspired by EPA’s voluntary “Energy star” mark.

Based on NIST IoT security recommendations, but developed by “Lead Administrator”, UL Solutions. *(China problems..)*

In USA only certain private organizations and business associations (in banking etc) *require* high-security products.

Even in govt., FIPS 140-3 still doesn’t require SCA or FIA resistance for any certification level, DoD NIAP is AVA_VAN.1.

The Cyber Resilience Act (CRA)

When we are working on the technical CRA standards, we frequently consult the CRA text itself (Especially Annex I, ***"Essential cybersecurity requirements."***)

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

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)

Annex I, Essential Cybersecurity requirements

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

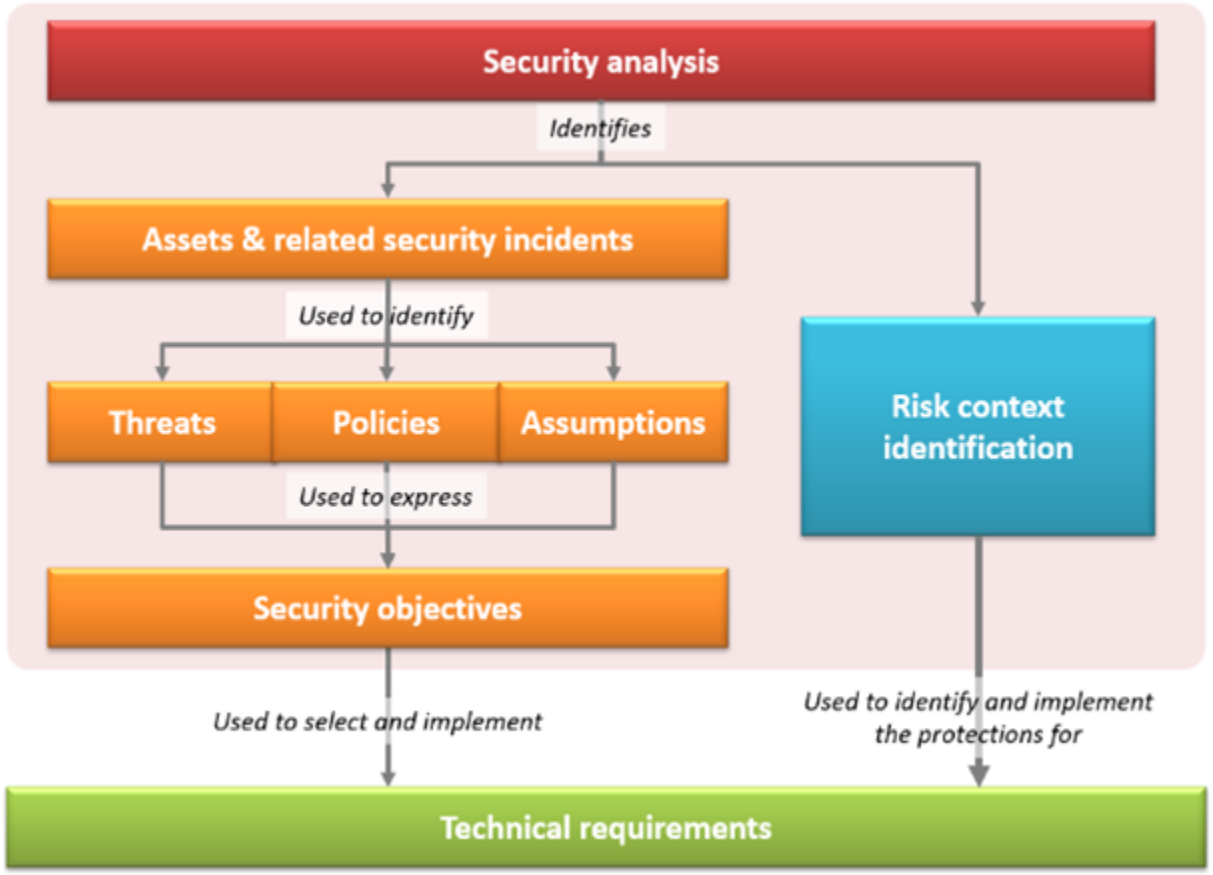
Addressed in JTC13 WG9 standards. Focusing on technical features in this talk.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

This point 2 has a list of 13 essential requirements, lettered from (a) to (m).

The risk assessment documentation should be included with the product.

Risk Assessment .. We're debating it



Annex I wording: the CRA Essential Requirements are "MUST" only if a risk assessment says so!

Traditional risk assessment is a list of risks, together with probability × loss.

With chips, the "loss" depends on how you use them – so some members want to make everything optional.

We'll see what kind of methodology is adopted. Some chip makers want to push risks analysis to integrators.

(a)..(d): Secure defaults, Update, Access Control

Secure “defaults” (requires intepretation for plain FPGAs..)

(a) *be made available on the market without known exploitable vulnerabilities;*

(b) *be made available on the market with a secure by default configuration,*

Need an **update mechanism**, which needs to be **automatic**.

(c) *ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates [..]*

Implement **access control**. Intrusive attacks / tamper are required elsewhere.

(d) *ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, [..]*

(e), (f): Cryptography is an Essential Requirement

Confidentiality (encrypting data at rest and data in transmit.)

(e) *protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;*

Data integrity (Hashes, MACs, and Signatures.)

(f) *protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;*

But.. what kind of crypto?

EN 18031 (RED): “Best Practice Cryptography” ?

The harmonized standards for the **EU Radio Equipment Directive (“RED”)** were ratified only last year (EN 18031-{1,2,3}) and do not force any specific crypto.

6.9.1.3 Guidance

There is various security guidance that can be used to identify best practices for cryptography, see respective ISO/IEC standards, publicly available crypto catalogues provided by SDOs and public authorities such as sogis.eu, “SOGIS agreed Cryptographic Mechanisms” [24], ETSI TS 119 312 Electronic Signatures and Infrastructures; Cryptographic Suites [42] and guidance provided by ENISA and national agencies as the NIST SP800 series [8]- [18] and BSI TR-02102-1[20].

A commonly used cryptographic method for a certain use case, with the lack of evidence for a feasible attack with current readily available techniques, can be considered as best practice.

However, it is also possible to provide evidence, that new cryptography is suitable for a certain use case and can therefore be considered as best practice for cryptography.

Best practice *until readily available exploits?*

EN 18031-{1,2,3} all say:

“A commonly used cryptographic method for a certain use case, with the lack of evidence for a feasible attack with current readily available techniques, can be considered as best practice.”

No foresight here. The use of known-weak crypto is "common".

In cryptography there is often ample warning of weaknesses.

Algorithmic vulnerabilities are rarely 0-days ..

VOLUME 2, NUMBER 2 — SUMMER 1996

RSA LABORATORIES'

CryptoBytes

The technical newsletter of RSA Laboratories, a division of RSA Data Security, Inc.

The Status of MD5 After a Recent Attack

Hans Dobbertin
German Information Security Agency
P.O. Box 20 03 63
D-53133 Bonn, Germany

Hash functions are frequently used cryptographic primitives. In digital signature schemes a message is hashed before signing. To prevent that by this interposition a weakness is generated, the applied hash function has to be collision-resistant. Hash functions also occur as components in various other cryptographic applications with usually much weaker requirements.

The hash function MD4 was introduced by Ron Rivest [15] in 1990. This was the starting point for

- strengthened versions RIPEMD-160 and RIPEMD-128 of RIPEMD, recently published by Bosselaers, Preneel, and the author [12].

Before 1995 collisions for two (of three) rounds of MD4 (den Boer and Bosselaers [5]), almost-collisions of MD4 (Vaudenay [17]), and pseudo-collisions for the compression function of MD5 (den Boer and Bosselaers [6]) had been found. In 1995 the author developed new methods to cryptanalyze MD4-like hash functions. In a series of attacks these techniques were applied on the first two and the last two (of three) rounds of RIPEMD, on MD4 in its entirety and the compression function of the 256-bit extension of MD4 (see [8-10]).

(g)..(k): System Design / Architectural

The following requirements are essentially design principles related to the minimization of sensitive data, availability, and reduction of attack surface.

(g) *process only data, personal or other, that are adequate, relevant and [..]*

(h) *protect the availability of essential and basic functions [..]*

(i) *minimise the negative impact by the products [..]*

(j) *be designed, developed and produced to limit attack surfaces[..]*

Mitigation of exploitation would probably mean e.g. isolation mechanisms.

(k) *be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;*

(l), (m): Logging, zeroization, and secure backups

Despite data minimization, there is a requirement for **logging** (with disable)!

(l) *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;*

The final requirement is about **zeroization** and **secure backups:**

(m) *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, ensure that this is done in a secure manner.*

Thank you!