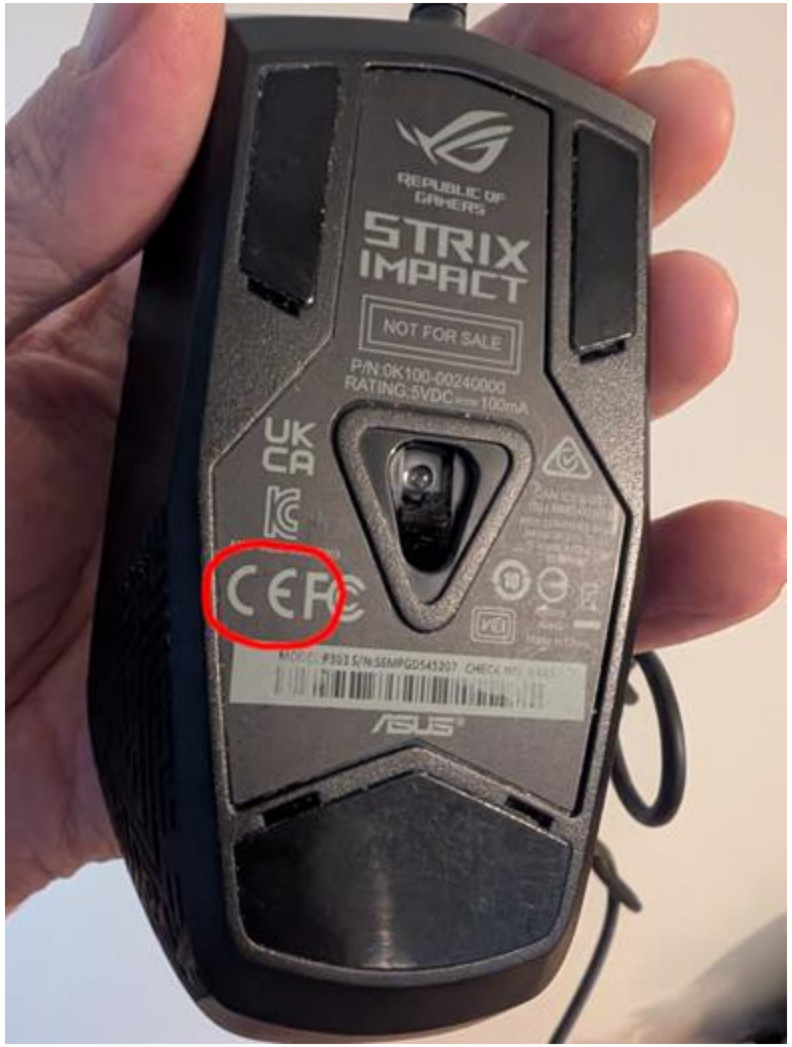
CRA and Cryptography
.. the story thus far

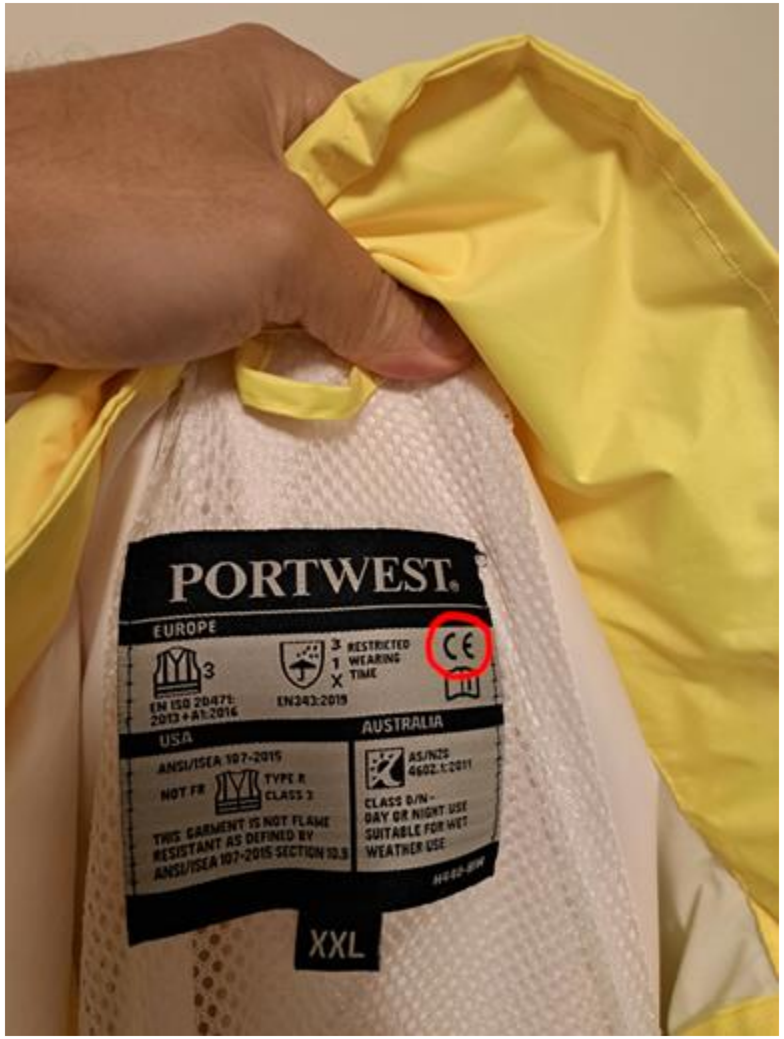
Markku-Juhani O. Saarinen
<markku-juhani.saarinen@tuni.fi>

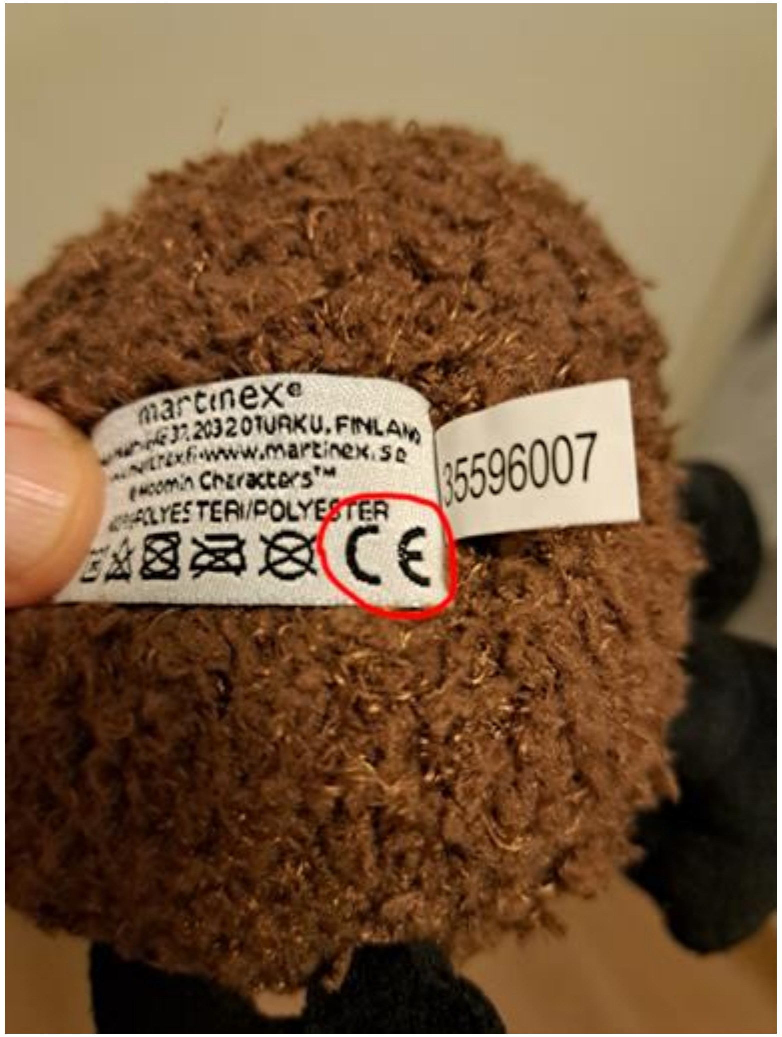
Loc & Date: Real World Crypto 2026
2026-March-10 Taipei, Taiwan

Tampereen yliopisto
Tampere University

My mouse? Raincoat? Plush toy?




PORTWEST.
EUROPE
3
EN ISO 20471:2013+A1:2016
3 1 X
RESTRICTED WEARING TIME
EN343:2019
CE
USA
ANSI/ISEA 107-2015
NOT FR
TYPE R CLASS 3
THIS GARMENT IS NOT FLAME RESISTANT AS DEFINED BY ANSI/ISEA 107-2015 SECTION 10.9
AUSTRALIA
AS/NZS 4602.1:2011
CLASS D/N - DAY OR NIGHT USE SUITABLE FOR WET WEATHER USE
XXL



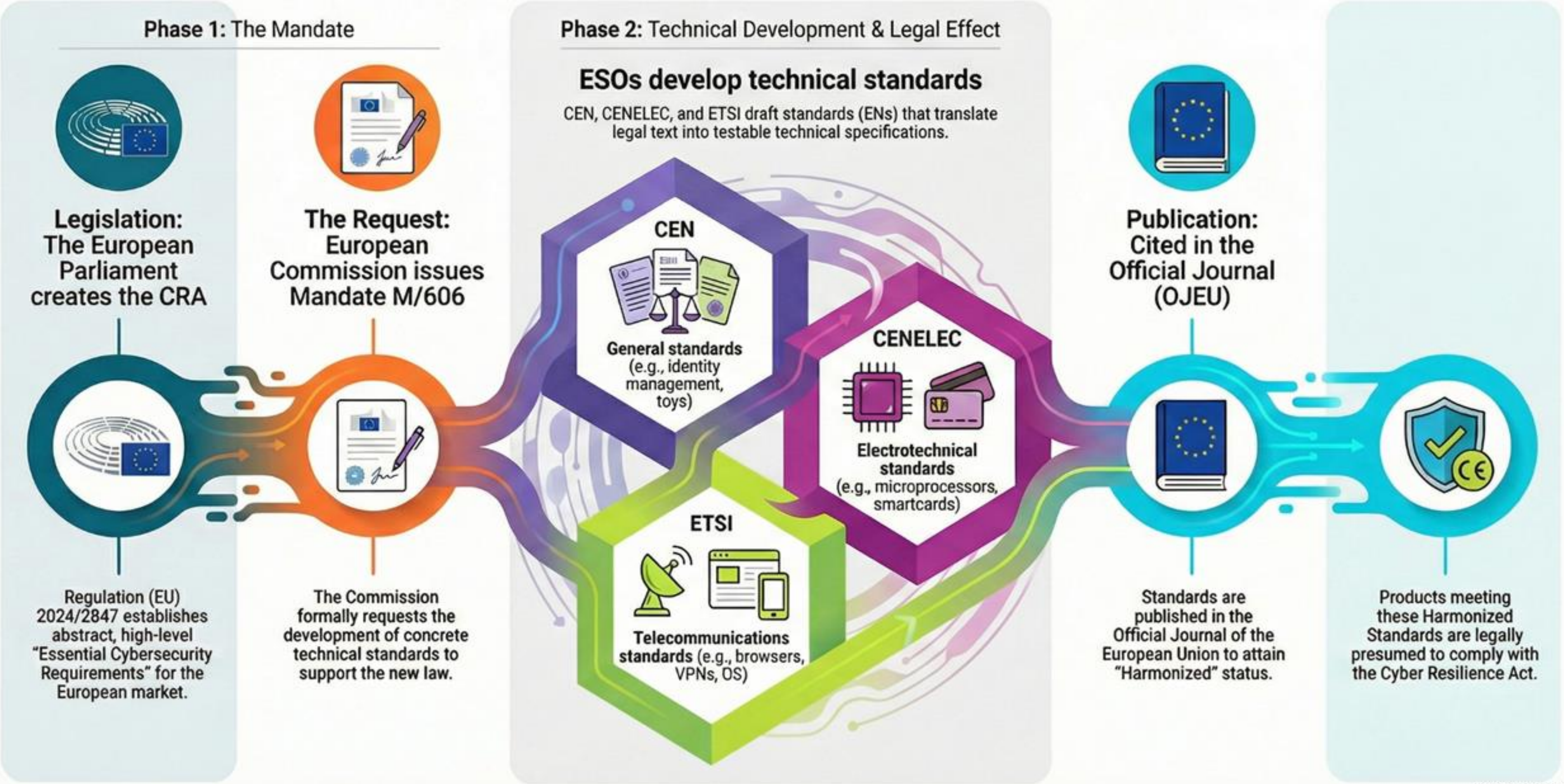
CRA: Cyber needed for the CE Mark

- Products affected by European safety/security regulations need a **CE mark** to be sold in the common market. Enforced by market surveillance.
- Requirements are defined in EU directive(s) / regulation(s) and **harmonized standards**.
- Compliance with **EU Cyber Resilience Act (CRA)** is **required** for CE mark from December 2027.

Official “**Blue Guide**” on the EU product rules:

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

The Path to Compliance: How European Cybersecurity Standards are Born



Phase 1: The Mandate

Legislation: The European Parliament creates the CRA

Regulation (EU) 2024/2847 establishes abstract, high-level "Essential Cybersecurity Requirements" for the European market.

The Request: European Commission issues Mandate M/606

The Commission formally requests the development of concrete technical standards to support the new law.

Phase 2: Technical Development & Legal Effect

ESOs develop technical standards

CEN, CENELEC, and ETSI draft standards (ENs) that translate legal text into testable technical specifications.

CEN

General standards (e.g., identity management, toys)

CENELEC

Electrotechnical standards (e.g., microprocessors, smartcards)

ETSI

Telecommunications standards (e.g., browsers, VPNs, OS)

Publication: Cited in the Official Journal (OJEU)

Standards are published in the Official Journal of the European Union to attain "Harmonized" status.

Products meeting these Harmonized Standards are legally presumed to comply with the Cyber Resilience Act.

ESOs = { CEN,CENELEC,ETSI }

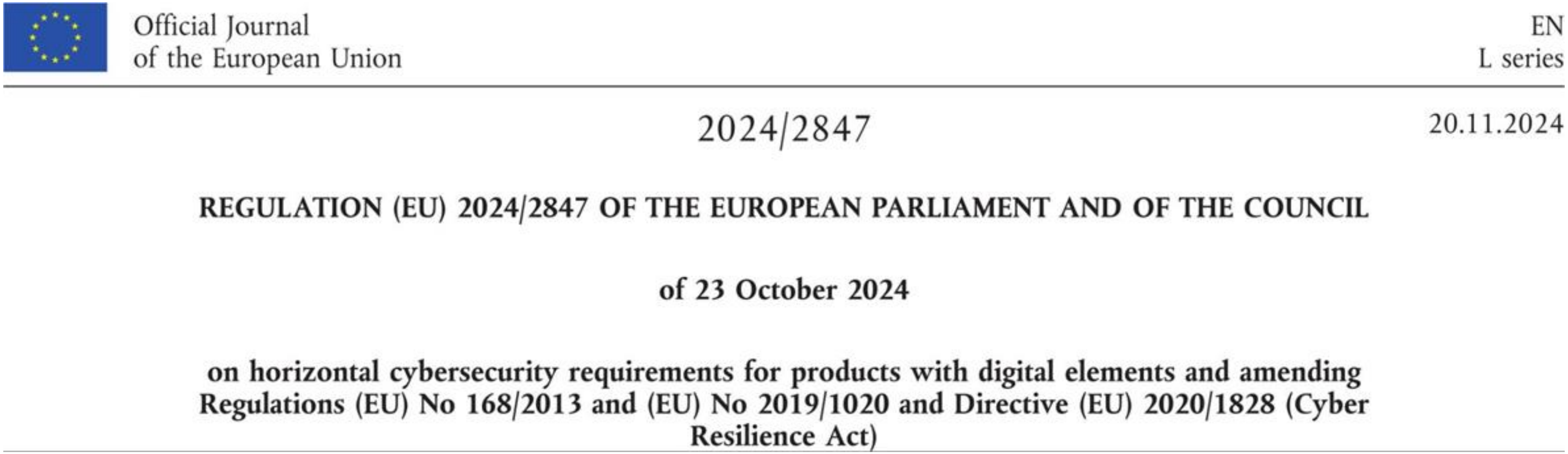
Background: In early 2025 I wanted to *read* the draft **CRA** harmonized standards from the European Standard Organizations (ESOs) **CENELEC**, **CEN**, and **ETSI**.

Not so simple: I had to get myself “appointed” there by my FI national std. orgs **SESKO**, **SFS**, and **TRAFICOM** ..

The Cyber Resilience Act (CRA)

When writing 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

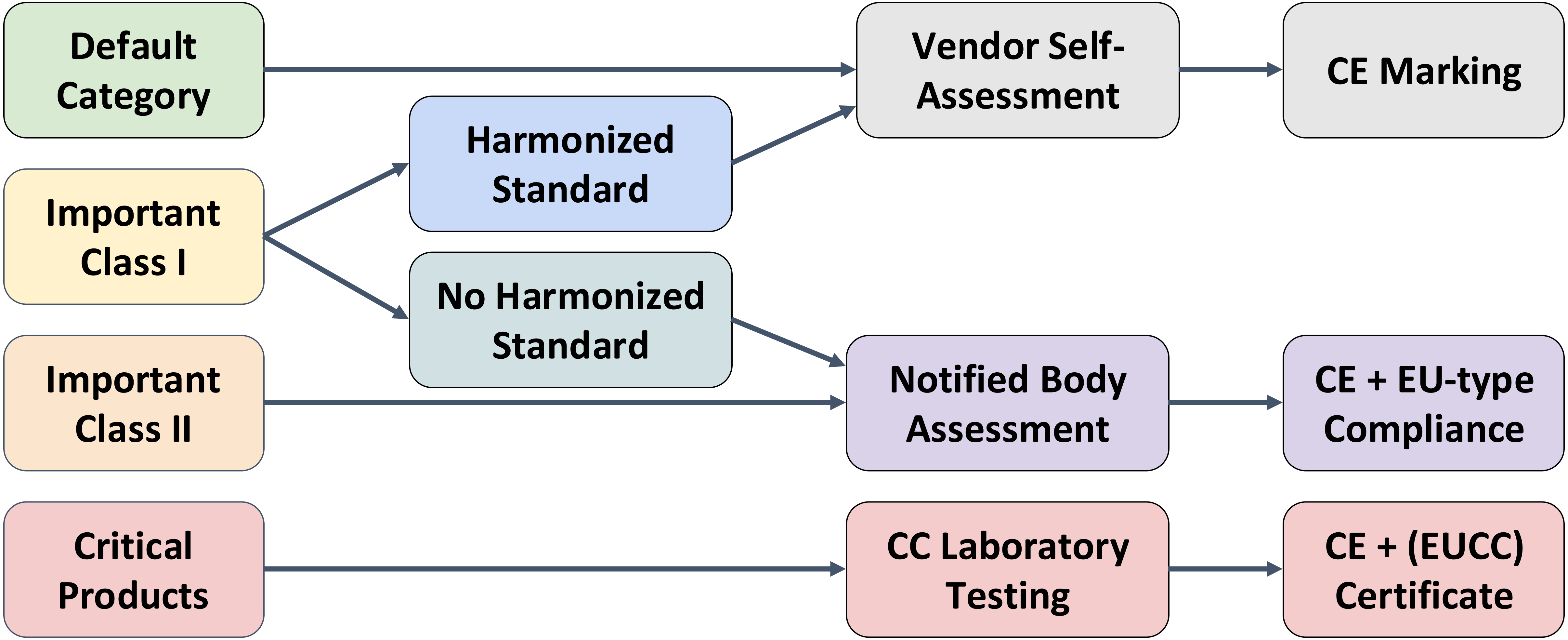
20.11.2024

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)

CRA Categories *(grossly simplified)*



Default Category: Self-Assessment

Software and hardware product **not** mentioned in Annex III are in the **CRA 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.*

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

“Important Class” standards..

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

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 horizontal standards:

Risk-based approach, Principles for cyber resilience, Generic Security Requirements, Vulnerability Handling, SBOM.

CLC/TC 65X WG 3 is developing additional vertical standards for CRA in the context of **Industrial Automation and Control**.

Main Cryptography Requirements

Confidentiality (encrypted communications and storage)

(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;*

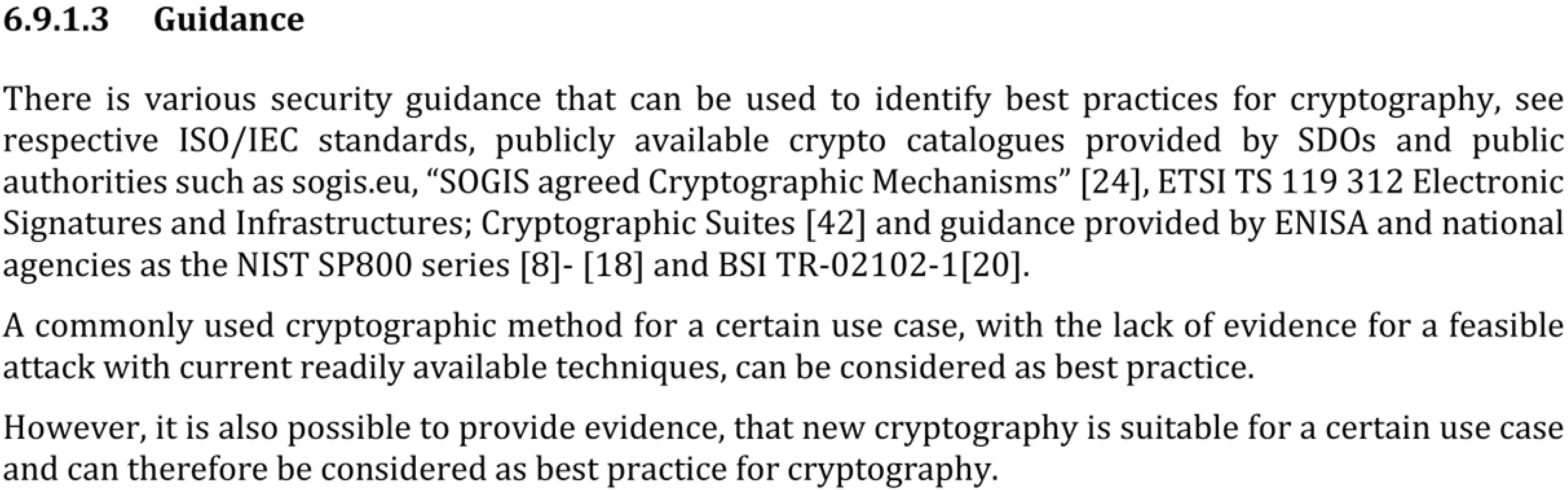
Data integrity (Hashes, MACs, and Signatures.)

(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?

RED: *“Best Practice Cryptography”*

The harmonized standards for the **EU Radio Equipment Directive** **<u>(“RED”)</u>** were ratified in 2024: EN 18031-{1,2,3}. (*But RED is now repealed/replaced by **CRA**.)*



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?*

<ins>EN 18031-{1,2,3} all say:</ins>

“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.

CRA Standards’ Annex K – Crypto

- Crypto is related to many/most Essential Cybersecurity Requirements:

  Part I-(2) (e) **confidentiality** (f) **integrity** directly, many other requirements indirectly require cryptography (secure updates, etc)

- Originally intended to be addressed by a horizontal standard (“PT2”). Vertical standards were starting to include their crypto reqs.

- Crypto “TF” uses ETSI templates and tools to create a normative Appendix **“K”** that rapporteurs/committees can choose to add to their standards.

ANNEX "K" IS UNDER INTENSE DISCUSSION RIGHT NOW AT ETSI-CEN-CENELEC

“State of The Art Cryptography”

- Define **State of the Art Cryptography (CRY-SOTA)** for **Secure Defaults.** (This is related to the language in ECR-I-2-e in the CRA Law.)

- CRY-SOTA: Publicly evaluated and standardized, technically up-to-date cryptographic mechanisms.

- Based on an *“allow list”* of cryptographic mechanisms from *“ECCG Agreed Cryptographic Mechanisms”* (**ACM**) and related future ECCG documents.

  https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

- Intended as a **Single Source of Truth**: We expect ACM to be accepted as a normative reference in harmonized standards.

What’s in “ACM” anyway? Not much..

The mechanisms listed ACM are considered “ok”, but in 2 classes:

1. **Recommended mechanisms**: Considered “state-of-the-art”.
2. **Legacy mechanisms**: Acceptable until a specified date.

Version 2.0 of ACM (April) 2025 had:

AES, 3DES, SHA2, SHA3, MAC modes, Key derivation, PBKDF2 *<- curious*

RSA, DSA, ECDSA (many variants), DH, ECDH *<- RSA < 3000 not allowed*

ML-KEM, FrodoKEM, ML-DSA, SLH-DSA, XMSS, LMS *<- FN-DSA, HQC-KEM ?*

TLS 1.2, TLS 1.3 (no IPSec or SSH) *<- need to add protocols*

SP 800-90A DRBGs (vague TRNG, does not mention 90B, 90C, AIS-20/31)

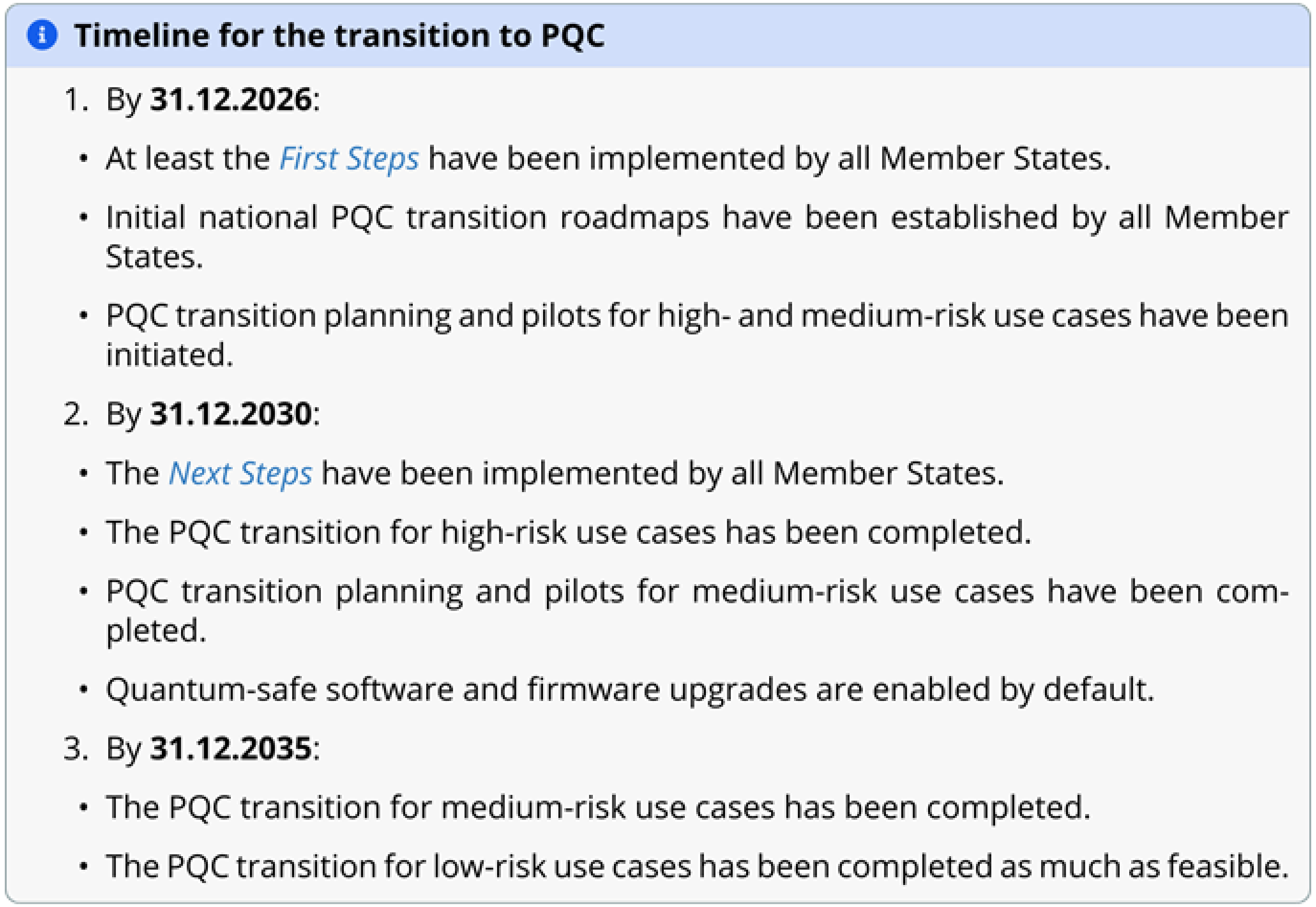
“Person Authentication” *<- this is lacking*

EU Coordinated Post-Quantum Roadmap

On 23 June 2025, EU member states and the commission: “**Roadmap for PQC transition**”

Specifically mentions CRA to address the PQC transition.

PQC transition dates can be addressed via the **recommended** vs. **legacy** structure in ACM.



Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography