

CRA and Cryptography: The Story Thus Far

Markku-Juhani O. Saarinen

[<markku-juhani.saarinen@tuni.fi>](mailto:markku-juhani.saarinen@tuni.fi)

Security Standardisation Research 2025
December 05, 2025 - Passau, Germany

OUTLINE

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

DISCLAIMER 1: I AM NOT A LAWYER. THESE ARE MY PERSONAL OBSERVATIONS.

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

DISCLAIMER 2: VERY PRELIMINARY INFORMATION, LIKELY TO CHANGE.

Preprint: <https://eprint.iacr.org/2025/2092>

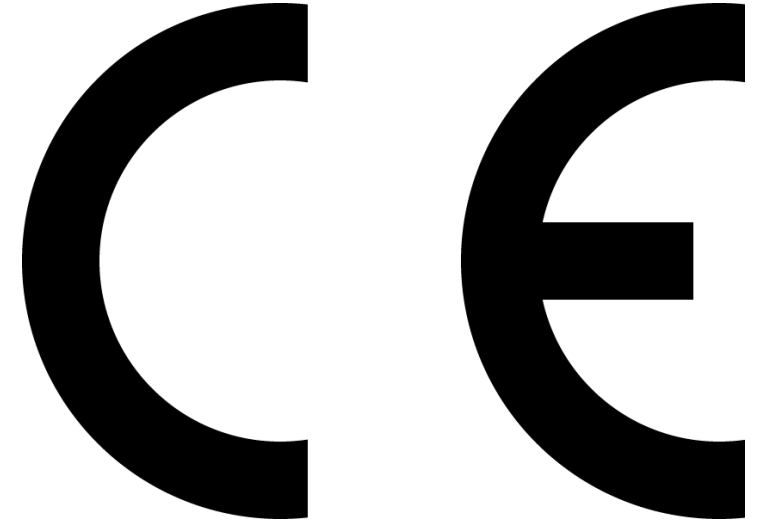
M.-J. O. Saarinen, *"CRA and Cryptography: The Story Thus Far"*

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

I live in Finland  . *My standards come from:*

		Electrotechnical industry	Other industries	Telecommunications industry
Global level		IEC International Electrotechnical Commission	ISO International Organization for Standardization	ITU International Telecommunication Union
European level		CENELEC European Committee for Electrotechnical Standardization	CEN European Committee for Standardization	ETSI European Telecommunications Standards Institute
National level		SESKO Electrotechnical industry	SFS Finnish Standards and its standards writing bodies	Finnish Transport and Communication Agency Traficom

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 Std. Orgs

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

A  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:

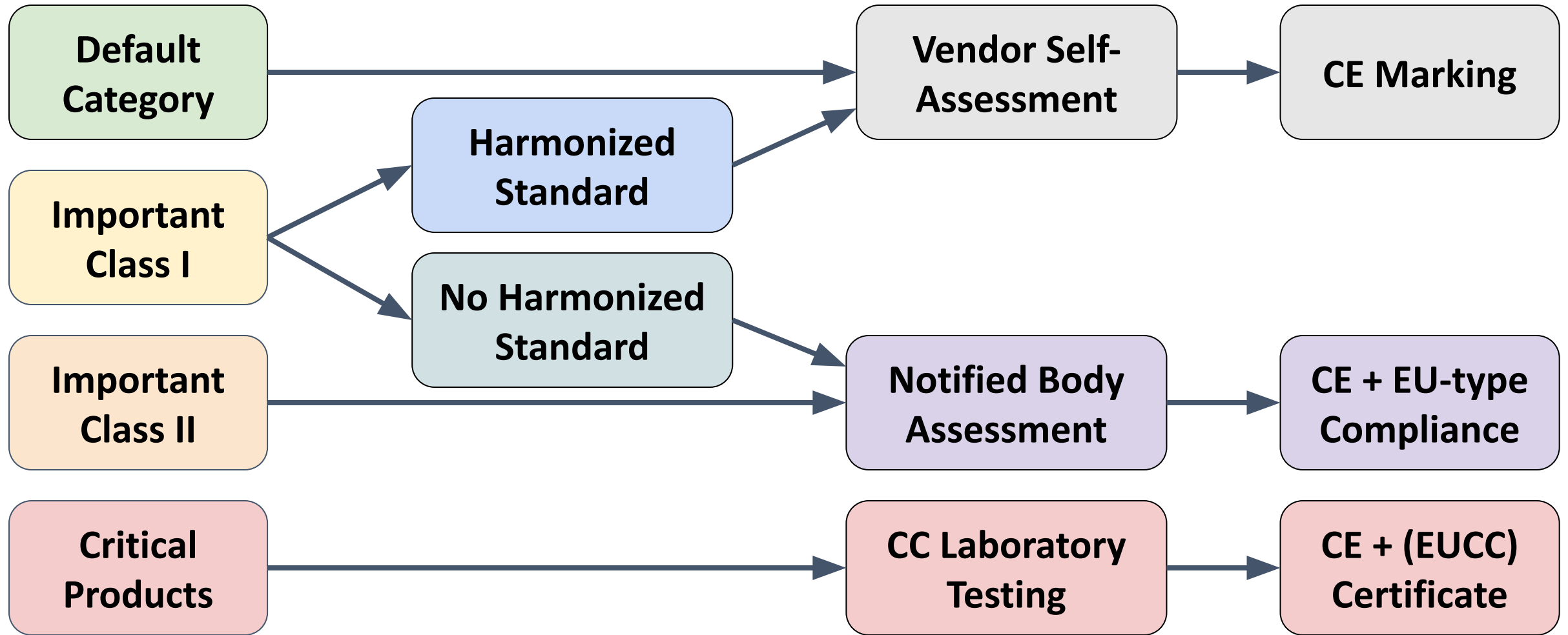
Almost no-one has visibility to the standards before they actually come out.

Only then they can be purchased for €50 .. €300 per 1 seat! (*who 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.



U.S. CYBER TRUST MARK



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.

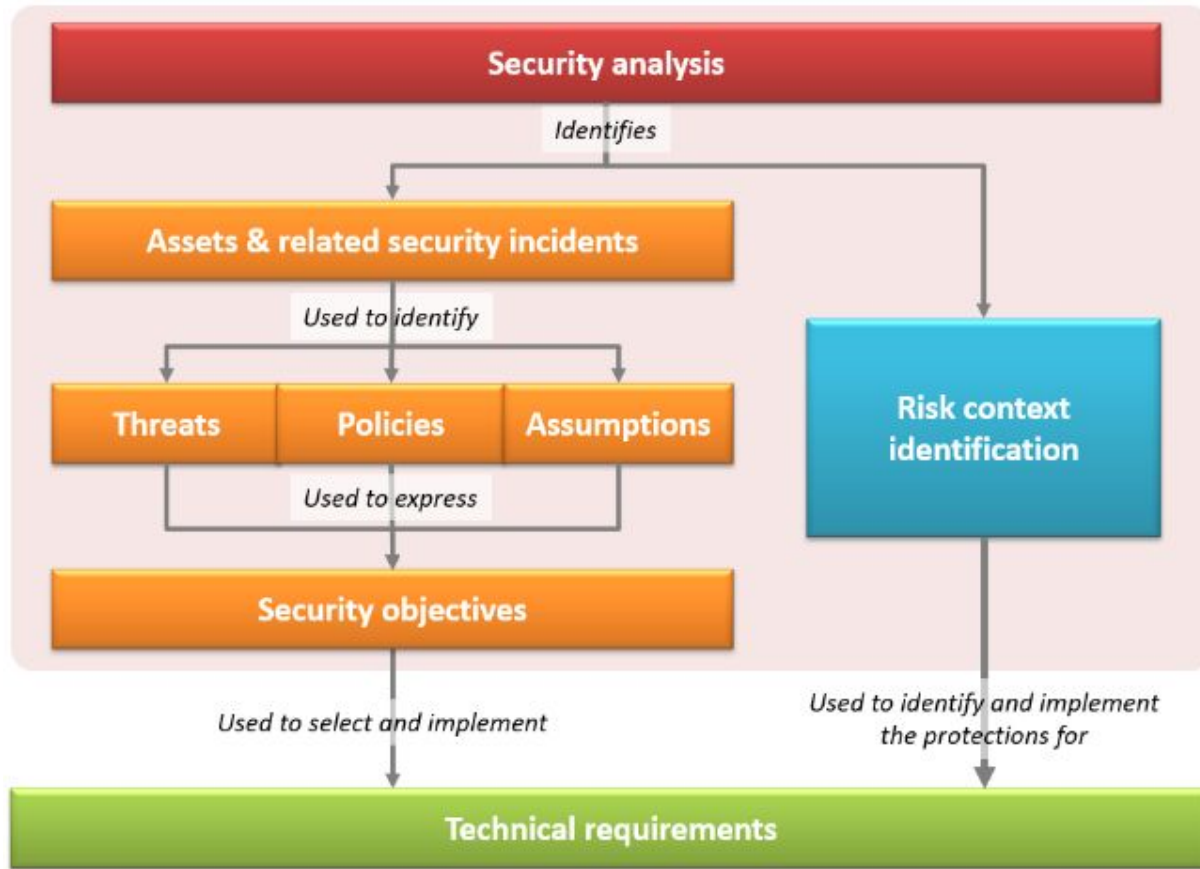
Addressed in JTC13 WG9 standards. Focusing on technical features in this talk.

(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 interpretation 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,

(more about cryptographic secure defaults later)

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): Main Cryptography Requirements

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]).

The screenshot shows a web browser window displaying the NSA Information Assurance website. The address bar shows the URL: https://www.nsa.gov/ia/programs/suiteb_cryptography/. The page header includes the NSA and Central Security Service logos, with the tagline "Defending Our Nation. Securing The Future." The navigation menu includes links for HOME, ABOUT NSA, ACADEMIA, BUSINESS, CAREERS, INFORMATION ASSURANCE, RESEARCH, PUBLIC INFORMATION, and CIVIL LIBERTIES. The main content area is titled "Cryptography Today" and discusses the importance of secure information sharing and the transition to quantum-resistant algorithms. A sidebar on the left lists various Information Assurance programs, including "Suite B Cryptography".

Information Assurance

- About IA at NSA
- IA Client and Partner Support
- IA News
- IA Events
- IA Mitigation Guidance
- IA Academic Outreach
- IA Business and Research
- IA Programs
 - Commercial Solutions for Classified Program
 - Global Information Grid
 - High Assurance Platform
 - Inline Media Encryptor
 - Suite B Cryptography
 - NSA Mobility Program
 - National Security Cyber Assistance Program
- IA Careers

Home > Information Assurance > Programs > NSA Suite B Cryptography

Cryptography Today

In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

(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;

(= crypto agility?)

(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.

2. "Brussels proposal" 06 Nov 2025

NOTE – VERY PRELIMINARY INFORMATION, LIKELY TO CHANGE

Crypto “Cross-Vertical” - Algorithms, Parameters

- Crypto is related to many/most Essential Cybersecurity Requirements: Part I-(2) (e) **confidentiality** (f) **integrity** directly, many others indirectly.
- Originally intended to be addressed by a horizontal standard (“PT2”). Cryptography vertical standards were starting to include their own versions.
- Crypto “TF” uses ETSI templates and tools to create a normative Appendix “K” that rapporteurs/committees can choose to add to their standards.
- The same text can also be adopted for other vertical standards.

Concept: State of The Art Cryptography

- Define a new concept of **State of the Art Cryptography** for **Secure Defaults**.
(This is related to the language in ECR-I-2-e. Old definition is a bit outdated.)
- 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
- **Single Source of Truth:** We expect ACM to be accepted as a normative reference in harmonized standards: Publicly evaluated and standardized, technically up-to-date cryptographic mechanisms to protect the security (esp. confidentiality and integrity) of user data, commands, and other relevant information in CRA.

What's in “ACM” anyway ?

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

1. **Recommended mechanisms:** Considered practical state-of-the-art.
2. **Legacy mechanisms:** Acceptable until a specific transition/sunset date.

Footnote: 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 <- *need RSA > 3000 bit from 31 Dec 2025*

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

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 Crypto Roadmap

On 23 June 2025, EU member states & the Commission issued a “roadmap for PQC transition”.

This document specifically recommends European cyber standardization (mentions CRA) to address the PQC transition.

The PQC transition dates will 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>

Risk Analysis: Impact for Crypto [suggestion]

Risk environment affects implementation **testing** but **not** recommended algorithms:

Important class 1 and 2: Functional tests (interop., test vectors), feature tests.

Critical class: Penetration test (at least AVA_VAN.3), can cover SCA, FIA, etc

Why? For two otherwise identical implementations (and modes, initialization, etc):

Key length: Risk(AES-128) \approx Risk(AES-256) *negligible probability difference*

But: Risk(AES Impl. 1) \gg Risk(AES Impl. 2) *can be a substantial prob. difference*

In cryptography one can argue that risk changes over time:

Risk(ECDSA) - Risk(ML-DSA) = grows over time, PQC compliance deadlines 2030, 2035.

ECDSA = Current signature standard, ML-DSA (Dilithium) = PQC Signature Standard

Secure Cryptographic Defaults

ECR I-2-(b): .. be made available on the market with a secure by default configuration.

Case A: “General purpose” intended use:

The cryptographic mechanisms used in the default configuration (“out of box”) to connect to the Internet shall be on the pre-approved “ACM” listing and shall be appropriate for the use (appropriate modes, initialization, hashes ≠ keyed macs, etc.)

Note: The use of harmonized standards is voluntary; Vendors who cannot meet these requirements can always go through a “notified body assessment” to put a product on the market. (*n. body = a third party evaluator approved by an EU government.*)

Business Intended Use allows non-ACM

ECR I-2-(b): be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements,

Case B: Tailored intended use:

The product is not intended for general Internet connectivity. The cryptographic mechanisms used in the default configuration (“out of box”) match those of a specific business or sector, and the mechanisms are documented with an appropriate reference.



(Just an example!)

We are not prohibiting other algorithms

For a number of reasons, it is not feasible to completely prohibit legacy or non-listed cryptography under a broad product legislation such as CRA:

1. There is a need to access (decrypt) legacy encrypted information, and to verify its authenticity and integrity using legacy mechanisms.
2. Devices must be able to communicate and interoperate with older devices and with devices in other regulatory frameworks.
3. There must be a way to introduce new cryptographic mechanisms into use without the need to insert them into ACM listings first.

Secure default configuration is a key concept in CRA (ECR I-2-b). Ultimately the user may configure any cryptography. In CRA the user is in control and there is an opt-out at least for security updates (ECR I-2-c) and logging (ECR I-2-l).

Cryptographic Agility Requirements

Rule: A product shall be able to technically support the cryptographic transitions announced in ACM (at least during its support period.)

Here is an attempt to articulate design goals (work in progress)

- 1. products shall have the capability to select their security algorithms flexibly, either via configuration or (for communication protocols) in real time, based on the combined security functions of communicating parties*
- 2. products shall have the ability to add new cryptographic mechanisms to existing hardware or software, resulting in new, stronger security features*
- 3. products shall have the ability to gracefully retire cryptographic mechanisms that have become either vulnerable or obsolete*

One possible agility test .. any further ideas?

In EN 303 645 “cryptagility” (provision 5-3-3) means that cryptography if applicable shall be “replaceable.” It is of course rather IoT - centric.

Todo: We can find neat design principles for crypto agility, but I have not yet worked out how to articulate such things in testable “verticals language”.

Note: In CRA products have a pre-specified minimum support period, and in ACM legacy algorithms have a retirement date.

Proposal: Require demonstrable cryptographic agility (to some alternative scheme, not necessarily the final replacement scheme used) if ..

- (a) .. the product has a legacy cryptography mechanism (as defined in ACM) as a default, and
- (b) the announced depreciation of that cryptographic mechanism occurs during the product’s support period.

Thank you!

Preprint: <https://eprint.iacr.org/2025/2092>

M.-J. O. Saarinen, *“CRA and Cryptography: The Story Thus Far”*

To appear: Security Standardization Research 2025 (04-05.12.2025)