CRA and Cryptography: The Story Thus Far

Markku-Juhani O. Saarinen

Information Security Laboratory, Tampere University, Finland
markku-juhani.saarinen@tuni.fi

Abstract. We report on our experiences with the ongoing European standardisation efforts related to the EU Cyber Resilience Act (CRA) and provide interim (November 2025) estimates on the direction that European cryptography regulation may take, particularly concerning the algorithm "allow list" and PQC transition requirements in products.

The CRA has a wide-ranging set of security requirements, including security patching and the use of cryptography (data integrity, confidentiality for data at rest and data in transit). However, the Cyber Resilience Act itself is a legal text devoid of technical detail – it does not specify the type of cryptography deemed appropriate to satisfy its requirements.

The technical implications of CRA are being detailed in approximately 40 new standards from the three European standardisation organisations, CEN, CENELEC, and ETSI. While the resulting ETSI standards can be expected to be available for free even in the drafting stage, the CEN and CENELEC standards will probably require a per-reader license fee. This, despite recent legal rulings asserting that product security and safety standards are part of EU law due to their legal effects. We outline some of the risks associated with the partially closed standardisation process, including active impact minimisation by vendors concerned with engineering costs, a lack of public review leading to lower technical quality, and an increased potential for backdoors.

Taking a recent (2024) example of cryptographic requirements in such standards, we observe that the definitions and language in the Radio Equipment Directive (RED DA) harmonised standard (EN 18031 series) may allow vendors to take an approach where weak cryptography is considered "best practice" right until exploitation is feasible.

Recognising recent developments such as the EU Post-Quantum Cryptography transition roadmap, many CRA standardisation working groups are moving towards a "State-of-the-Art Cryptography" (SOTA Cryptography) model where approved mechanism listings are published by the European Cybersecurity Certification Group (ECCG). CRA-compliant products may still support other cryptographic mechanisms, but only SOTA is permitted as a safe default for Internet-connected products.

Keywords: CRA – Cyber Resilience Act · RED-DA · Agreed Cryptographic Mechanisms · Cryptographic Agility · PQC Transition

1 Introduction

Our research interest in Cyber Resilience Act (CRA) standardisation was initially motivated by a simple desire to "find out" about its potentially huge implications on cryptography and product security testing in Europe. However, it soon became apparent that there were no public working documents, discussion forums, and very few open sources with detailed technical information.

Even after the standardisation process is finished, CEN and CENELEC standards in particular are not freely available, and their contents are protected by copyright. In our experience, a rather common attitude in cybersecurity engineering is to ignore such technical standards. Paywalled, per-seat licensed documents are challenging for actual cybersecurity engineering and testing teams to use. However, due to the wide-ranging and legally binding obligations of the CRA regulation, these particular standards can't be easily dismissed.

Due to lack of transparency, studuing the CRA security standards requires "participatory fieldwork". A security researcher must invest time and effort to gain access to the institutions and participate in the processes to gain technical information. This work is primarily based on subjective observations as a national expert and as an interim rapporteur of one of the vertical standards.

At the time of writing, the standards are not yet finished, so the reader must understand that all information contained herein is preliminary. Furthermore, it is essential to note that the author is not a legal expert. This work should not be interpreted as a legally accurate description of the rules and regulations governing the creation of standards, but as a subjective description.

Structure and Contributions. Section 2 contains a brief introduction to the European product legislation system and harmonised standards, and also offers a critique of the practical and security implications of the relatively closed standardisation process. Section 3 discusses the contents of the Cyber Resilience Act in the context of cryptography and the upcoming cybersecurity standards. Section 4 discusses cryptographic requirements in the related Radio Equipment Directive Delegated Act (RED-DA) standards (EN 18031) from 2024; we focus on an apparent "best practice loophole" in its wording, which can allow weak cryptography. This is followed by a discussion of cryptography in CRA (Section 5) and the proposed "State-of-the-Art Cryptography" concept and its "allow list" approach, which mainly determines the methods allowed in "secure default" settings of self-assessed products. We conclude in Section 6.

2 CRA and EU Product Regulation: A Crash Course

On 10 December 2024, the EU Cyber Resilience Act (CRA) [13] entered into force. The main obligations introduced by the Act will take effect on 11 December 2027. Compliance with this law would be required to sell "products with digital elements" (most types of software and consumer electronics) in the European common market of 450 million people. Compliance with CRA is needed to obtain the “CE-mark” (See Fig. 1) that is required in electrical gadgets, raincoats, toys, industrial machinery, and many other classes of products to be sold in Europe.

The CE-mark (from “Conformité Européenne”) means that the product conforms to relevant European regulations – whatever they may be for that particular product. It is not a “Made in Europe” mark, nor does it necessarily indicate that the product is of particularly high quality. CRA is just the latest addition to a long list of regulations that consumer electronics and many other types of products must meet to have the CE mark; they must be safe for the voltages that they use, should not cause electromagnetic/radio interference, etc. The general product rules are laid out in the “Blue Guide” [10], which has traditionally been one of the most essential references for compliance engineers. The Blue Guide is crucial when interpreting the implications of the CRA, as it also describes many relevant concepts and legal mechanisms such as *“market surveillance”* – the actual monitoring and enforcement of these European product regulations.

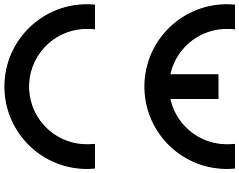

Fig. 1. The CE mark is required to sell many kinds of consumer products, including almost any kind of electrical device, on the European single market. CRA compliance will be a requirement for the CE mark from 2027.

2.1 European Standards and Harmonised Standards

European standards carry an EN number and have the format EN [number]:[year]. There are three European standardisation organisations[*]:

- European Committee for Standardisation (CEN)
- European Committee for Electrotechnical Standardisation (CENELEC)
- European Telecommunications Standards Institute (ETSI)

The areas of work of CEN, CENELEC, and ETSI generally mirror the international organisations (largely unrelated to CRA – here just for completeness):

- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union (ITU)

Broadly speaking, electrotechnical matters are in the scope of IEC/CENELEC, ITU/ ETSI handles telecommunication matters, while ISO/CEN addresses the remainder. Most European countries also have a matching national layer that can specify national standards (Fig. 2), which also forms the representation on upper layers (European and International). There are significant areas of overlap, resulting in joint ISO/IEC (CEN/CENELEC) standards in particular.

[*] The roles of CEN, CENELEC, and ETSI are laid out in Regulation (EU) No 1025/2012 of 25 October 2012 on European standardisation. `https://eur-lex.europa.eu/eli/reg/2012/1025/oj/eng`

	General	Electrotechnical	Telecomms.
International	ISO	IEC	ITU
European	cen	CENELEC	ETSI
National *(Example: Finland)*	SFS Suomen Standardit	SESKO	TRAFICOM Liikenne- ja viestintävirasto

Fig. 2. The division of duties between the three main international standardisation organisations ISO (General), IEC (Electrotechnical), and ITU (Telecommunications) is reflected on the European level (CEN-CENELEC-ETSI), and often even on the national level. The three national standardisation organisations of Finland are given as an example, but each of the 27 EU member states has its own national organisations.

A *harmonised standard* is a standard from CEN, CENELEC, or ETSI that is a result of a standardisation request from the European Commission**. The publication of a reference to a harmonised standard in the Official Journal of the European Union (OJEU) gives it a specific legal status, *presumption of conformity*. This means that if a product fully complies with the technical requirements of a harmonised standard, it is also presumed to be compliant with the related product regulation (e.g., safety or security laws).

2.2 Participation in CEN and CENELEC

In theory, the standardisation bodies operate within a system where national standardisation bodies (in each of the 27 European Union member states) select representatives to work on the European and international levels. However, the opportunities for participation vary significantly from one country to another. Based on our observations, a majority of the 27 EU countries do not have even a single active participant in the CRA standards-writing process, even though the standards form a part of the ruleset that affects everyone in Europe.

While ETSI has adopted an open policy regarding CRA standard drafts and other working documents, the distribution of CEN and CENELEC documents tends to be strictly limited to members of the relevant working groups.

** A list of harmonised standards: `https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/harmonised-standards_en`

In practical terms, one often has to first pay a fee to participate in the national standardisation group (in the author's case, 600 € for SESKO membership to monitor the CENELEC TC 47X group, responsible for semiconductor security), and then ask the national standards body or industry association to appoint oneself as a representative on the European level. Large companies do this routinely to protect their interest in the standardisation front. In the particular case of the author, the Finnish associations were supportive of academic representation, but most European experts will face significant difficulty accessing CEN and CENELEC drafts.

2.3 Accessing the Final Standards

While the ETSI CRA standards (the majority of the software-oriented CRA vertical standards) are expected to be publicly available (and some already are, in draft format: `https://www.stan4cra.eu/etsi-tc-cyber`), the cybersecurity standards being developed by CEN and CENELEC are not expected to be available for free. As can be seen in Table 1, this would primarily impact the horizontal standards (that are somehow intended to assist all European product vendors), and also chip standards from CENELEC.

The standards continue to be non-free despite harmonised standards forming an integral part of the regulatory framework for the European internal market[⋆⋆⋆] This has been recognized in a recent judgment by the Court of Justice of the European Union on the free availability of CEN standards related to the safety of toys.[†] It appears that fundamental changes in the standardisation system are required to overcome this restriction.

While the price point of standards is not overwhelming, it remains prohibitive for casual review or everyday use. Almost all European standardisation bodies sell the same English-language standards, but with wildly varying prices. Let us take the RED-DA standard EN 18031-1 as an anecdotal example: Checking for the cost of a 1-seat licence in October 2025, the price ranged from 43.72 € in Lithuania (LVS), to 161,00 € in Finland (SFS), and 327,70 € in Germany (DIN).

Even if a copy of the standard is purchased, its license prohibits the passing of the standard text to colleagues; hence, ISO, IEC, CEN, and CENELEC cybersecurity standards are difficult to reference in engineering specifications. In fact, it has been argued that it is best practice not to use closed (non-free) standards in security engineering as it prohibits open review (related to Kerckhoffs' principle [4] in cryptography.)

[⋆⋆⋆] This system originates with the so-called "New Approach" Council Resolution of 7 May 1985, `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31985Y0604(01)`

[†] Court of Justice of the European Union press release on 5 March 2024: "Judgment of the Court in Case C-588/21: The European harmonised technical standards on the safety of toys should be accessible to EU citizens." `https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp240041en.pdf`

By comparison, NIST has worked through open competitions to create the well-received cryptographic standards [23] that Europe has also included in its ACM listing [7]. From a European perspective, it is relatively easy to have faith in these algorithms thanks to the transparency of the NIST process and the historical fact that European academic researchers were strongly involved in the design of many of them. Apart from a few exceptions, their design criteria are well-known. For cryptographic protocols (such as TLS and IPSec), the IETF creates standards via an open consensus method driven by individuals (the IETF doesn't even have formal membership). Both NIST and IETF standards are freely distributed.

2.4 Security Risks in the CEN-CENELEC Process

As discussed, European citizens have very limited opportunities to review and influence CEN and CENELEC harmonised standards before they take legal effect – and afterwards, the standards are only available for a fee. Due to their licensing fee structure, they are not generally available even in academic libraries. There are obvious risks stemming from such a lack of transparency when developing what, in effect, is a legally binding security regulation.

We will list some information security and operational risks we have observed in the current CEN-CENELEC standardisation process (and to a somewhat lesser degree, in the ETSI processes), which would be significantly reduced if the process were made more open and transparent.

Vendors participate in the process solely to minimise the impact of security standards. Particularly CEN and CENELEC standardisation working groups are generally composed through nominations from national industrial bodies. These are commercial entities – the primary goal for some companies is to simply minimize the impact of CRA on their product lines and the need for costly security engineering. While the technical input from the industry is welcome to help arrive at workable standards, there should be a balance that prevents committee members with apparent conflicts of interest from rendering security standards ineffective.

Limited public review leads to low quality. Trust in cryptographic mechanisms is almost entirely derived from the amount and the quality of review they have received. The participation of scientific experts in CEN and CENELEC work, even in the development phase, is challenging, as non-public work is contrary to their performance indicators and the principles of open science. The lack of expert participation and critical review leads to lower-quality standards.

Potential for security backdoors. The infamous example of the "Dual EC" cryptographic back door [3] (and possibly others [6]) contained in the ISO/IEC 18031 [14] (not to be confused with EN 18031!) Random Bit Generator standard emphasizes that not only must the final standards be available for public review, but their entire design process, origins, and selection criteria must also be publicly disclosed. This does not happen in the closed process.

3 CRA's Essential Cybersecurity Requirements

One of the main functions of the CRA harmonised standards is to codify an interpretation of *Essential Cybersecurity Requirements* (ECR) contained in Annex I of the CRA law itself [13]. The ECRs are structured into two parts:

Part 1: Cybersecurity properties of the products. There are two main technical requirements in this part. The first one is a catch-all: *"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."*

The second requirement (ECR P1-2) is divided into a list of 13 technical points, (a) to (m), all of which are applied "on the basis of the cybersecurity risk assessment". The main cryptographic requirements are:

(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*

(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*

There are further requirements that less directly require the use of cryptography, including (c) on automated updates, (d) on authentication, (l) on logging, and (m) on secure erase and backup. The technical interpretation of all of these requirements is left to the harmonised standards.

Part 2: Vulnerability handling requirements. The draft horizontal standard on vulnerability handling requirements (known as Work Item JT013090) has normative dependencies on existing standards EN ISO/IEC 30111 ("vulnerability handling processes") and EN ISO/IEC 29147 ("Vulnerability disclosure"), and generally follows the procedures outlined there. This standard is expected to have a presumption of conformity in relation to vulnerability handling.

Technical cryptographic requirements are generally outside the scope of Part 2, although the standard is likely to include secure communication requirements for vulnerability information. The underlying standard (EN ISO/IEC 29147:2020 clause 5.8.2) has references to TLS, S/MIME, and OpenPGP as potential tools for this task.

3.1 Interpreting the ECRs

While the language around "confidentiality" and "integrity" ECRs appears unambiguous, they are dependent on a risk assessment. Some vendors in the standardisation groups have an interpretation that allows the risk assessment to be used to escape relatively costly updates of their product lines. To support such a claim, a vendor would have to demonstrate that the risk arising from the use of weak, proprietary, or legacy cryptographic methods is so low "in practice" that their use is acceptable under the Cyber Resilience Act.

Vendors can always try this tactic in a third-party assessment with *notified bodies* (independent third-party conformance evaluation bodies accredited by

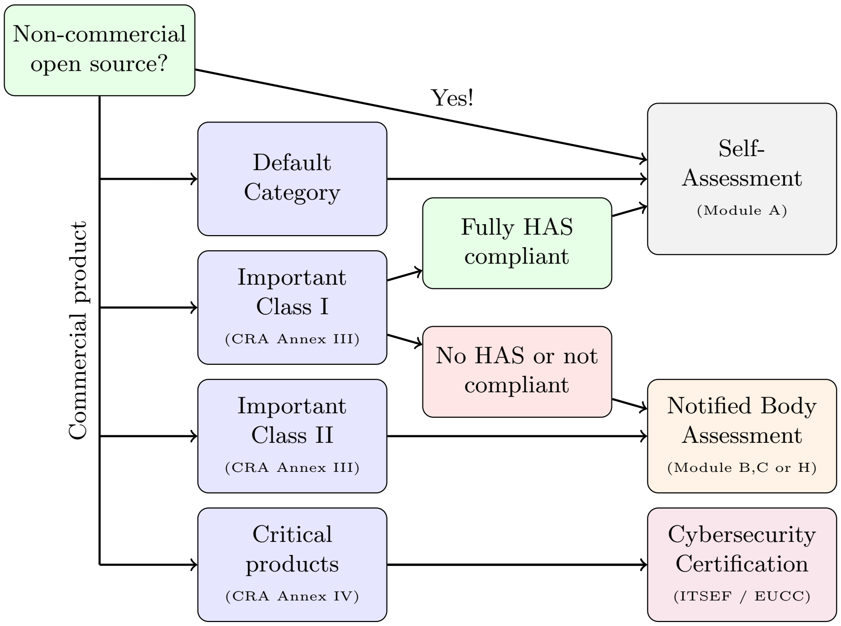

Fig. 3. Typical paths for (presumption of) conformance for various CRA product categories. The vast majority of products are in the "default category" – vendors can place a CE mark on their products after a self-assessment if they meet all relevant requirements. For Important Class I, "HAS" refers to a vertical harmonised standard with a presumption of conformity.

member countries). It remains to be seen under what conditions such claims of "low-risk bad cryptography" will be successful – the notified bodies will utilise relevant harmonised standards, document review, and product tests for the determination.

An important question arises about what kind of risk assessment (and resulting selection of cryptographic mechanisms) will be considered valid in self-assessment (internal control) – after all, the majority of products are expected to receive their CE mark this way. The relevant harmonised standards will also determine this. The monitoring of self-assessments (and the possibly resulting enforcement actions) will be left to market surveillance authorities after the product is already placed on the market. Market surveillance should utilise the same rules and standards as the notified bodies.

3.2 CRA Product Classes

CRA Annexes III and IV have lists of product categories that can be used to establish if a third-party assessment is required, and what type of assessment is sufficient:

- **Default category**: Low risk usage where self-assessment can be used. The expectation is that the vast majority of products are in this category.
- **Important Class I**: Products listed in CRA Annex III, where self-assessment suffices if the European Commission has approved a suitable Harmonised Standard, and the product is fully compliant with its requirements.
- **Important Class II**: Products listed in CRA Annex III, where compliance is assessed by a Notified Body based on evidence from the vendor.
- **Critical products**: The use of a European Cybersecurity Certification Scheme is expected. Currently, the only such scheme is the EUCC [11] Common Criteria-based scheme.

Fig. 3 shows some common pathways through the compliance process for various product categories. For an indication of various products in each class, see the listing of vertical standards in Table 1. There are many complications and additional rules to the decision diagram, so this figure should not be considered complete.

3.3 The CRA Standardisation Request

The European Commission issued a standardisation request[‡] related to CRA to European standardisation agencies in February 2025. There are two main kinds of standards in the standardisation request:

- **Horizontal standards** which apply to a wide range of products; in the case of CRA, essentially all products are under their scope, but "default category" standards in particular are impacted by horizontal standards.
- **Vertical standards** which are more specific, and generally tied to the product classes in Annexes III and IV in CRA (see Section 3.1).

An annex to the standardisation request listed 41 different items for standardisation. CEN, CENELEC, and ETSI then divided this enormous standardisation task among their Technical Committees (TCs) and Working Groups (WGs) – some requested standards were combined while others were further split into separate standards.

The standardisation request resulted in the work programme M/606[§] that is currently being executed by the standardisation bodies. Table 1 contains a preliminary (and still partial) list of standards currently being developed at ETSI, CEN, and CENELEC.

[‡] The 3 February 2025 European Commission Standardisation Request related to CRA (and its annexes) is available from: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en

[§] CEN, CENELEC and ETSI Work Programme M/606, dated 2 Apr 2025: https://www.cencenelec.eu/media/CEN-CENELEC/News/Newsletters/2025/m_606_work_programme_final.pdf

Table 1. A list of draft (CEN-CENELEC) horizontal standards and a rough mapping from the product classification in CRA [13] Annexes to related vertical standards under development at ETSI, CEN, and CENELEC, based on information available in November 2025. All of the standards are works in progress.

Horizontal Standards: CEN-CENELEC JTC 13/WG 9
(October 2025 development status of drafts.)

Std Number	Work Item	Status	Title
EN 40000-1-1	JT013095	ENQ	Vocabulary
EN 40000-1-2	JT013089	ENQ	Principles for cyber resilience
EN 40000-1-3	JT013090	ENQ	Vulnerability Handling
EN 40000-1-4	JT013091	On hold	Generic Security Requirements
TR 40000-1-5	JT013097	On hold	Threats and Security Objectives

CRA Annex III, “Important Class I” Verticals

1.	CEN	(Line 16)	Identity and privileged access management products.
2.	ETSI	EN 304 617	Standalone and embedded browsers.
3.	ETSI	EN 304 618	Password managers.
4.	ETSI	EN 304 619	software that searches for, removes, or quarantines malicious software (“anti-virus”.)
5.	ETSI	EN 304 620	Virtual Private Networks (VPNs) (parts 1 and 2).
6.	ETSI	EN 304 621	Network Management systems.
7.	ETSI	EN 304 622	Security information and event management (SIEM).
8.	ETSI	EN 304 623	Boot managers.
9.	ETSI	EN 304 624	PKI 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, internet modems, switches.
13+14.	CLC	EN 50765	CPUs and MCUs (low-risk environment.)
15.	CLC	EN 50767	ASICs and FPGAs with security functionalities.
16.	ETSI	EN 304 631	Smart home general-purpose virtual assistants.
17.	ETSI	EN 304 632	Smart home products with security (locks, cameras, baby monitoring, alarm, ...)
18.	ETSI	EN 304 633	Internet-connected toys (interactive features or tracking).
19.	ETSI	EN 304 634	Personal wearables (health monitoring, tracking)

CRA Annex III, “Important Class I” Verticals

1.	ETSI	EN 304 635	Hypervisors and container runtime systems.
2.	ETSI	EN 304 636	Firewalls, intrusion detection, and/or prevention.
3+4.	CLC	EN 50766	CPUs and MCUs (higher-risk: “tamper-resistant.”)

CRA Annex IV, “Critical” Verticals

1.	CEN	(Line 39)	Hardware devices with security boxes.
2.	CEN CLC	(Line 40)	Smart meter gateways within smart metering, secure cryptoprocessing.
3.	CLC	EN 50764	Smartcards or similar devices, secure elements.

Note: Six additional standardisation items that apply CRA to industrial automation and control systems and their networks are being developed by CLC/TC 65X WG 3.

4 Cryptography and the Radio Equipment Directive

One of the main models for the development of the CRA standards is the EN 18031-{1,2,3} series [17,18,19] of harmonised standards related to the Radio Equipment Directive Delegated Act (RED-DA)[¶]. Since August 1, 2025, manufacturers placing radio equipment on the European market have been required to comply with the requirements of RED-DA.

Somewhat similar to the CRA (but with a smaller scope), RED is part of European product regulation and includes cybersecurity requirements. The scope of the earlier RED regulation is essentially a subset of products covered by CRA. The EN 18031 harmonised standards [17,18,19] can be used for conformity self-assessment with some caveats[‖].

Many of the RED cybersecurity requirements imply the use of cryptographic mechanisms, so-called "[CRY-1] best practice cryptography." The EN 18031 standards offer guidance for this, including references to relevant NIST, BSI, and SOG-IS documents. However, each EN 18031 standard also contains the following characterisation:

> *"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."* – EN 18031-{1,2,3} [17,18,19]

A vendor performing self-assessment can interpret this statement (or definition) to mean that a cryptographic mechanism with known weaknesses or potential vulnerabilities can be considered "best practice cryptography", as long as others also use it and the exploits are "difficult" or not readily available.

This definition is close to the one used in ETSI IoT Cybersecurity standard EN 303 645 [8]. Although its assessment specification, ETSI TS 103 701 [9], encourages the use of SOG-IS reference catalogues (a predecessor to current ECCG catalogues [7]), it also allows arbitrary algorithms based on "competent cryptanalytic reports" from vendors. ETSI TS 103 701 is primarily designed for independent Testing Laboratories (TL) and notes that *"The competence of the TL has a strong influence on the validity of the assessment results."* [9]. Its use in CRA self-assessment seems especially hazardous, with vendors potentially self-approving arbitrary (or even proprietary) cryptographic mechanisms.

Typically, cryptographic methods are known to be vulnerable long before exploitation with "current readily available techniques" starts. A prominent example is the SHA-1 hash function, which was considered cryptanalytically broken by 2005 [24] but remained in use even after practical attacks were demonstrated in 2017 [22].

To most cryptographers, the no-foresight "currently feasible attack" approach allowed by EN 18031 represents the opposite of what would be considered best

[¶] RED-DA: Commission Delegated Regulation (EU) 2022/30 of 29 October 2021. `http://data.europa.eu/eli/reg_del/2022/30/2023-10-27`

[‖] In OJEU, the European Commission imposed limitations to presumption of conformance when using EN 18031 standards, but those are not related to its "best practice cryptography": `http://data.europa.eu/eli/dec_impl/2025/138/oj` practice. In the case of encryption, the implied approach contradicts policies such as the EU Post-Quantum Cryptography Transition Roadmap [12] (quantum computers are not "readily available") and the well-known "store now, decrypt later" threat model, which is unique to confidentiality protection.

5 CRA Cryptography and Harmonised Standards

We emphasise that no binding decisions have been taken on CRA cryptologic matters at the time of writing; this section simply reflects information and the status of the proposals as it is available to the author at the time of writing.

5.1 Defining "State of the Art"

The standardisation request[**] states that the resulting standards shall reflect the generally acknowledged state of the art, with a further explanation in a footnote:

> *"The state of the art does not necessarily imply the latest scientific research still in an experimental stage or with insufficient technological maturity. The state-of-the-art is not to be intended as minimum requirements to access the market."*

Based on discussions with the European Commission, the RED-DA "Best Practice Cryptography" approach, or at least its wording (Section 4), is being recognized to be insufficient to meet the criteria set in the CRA standardisation request. Since it is difficult to change definitions that are already in harmonised standards, and the language in the CRA Annex I confidentiality requirement ECR P1-2-e (Section 3), a new concept of practical "State-of-the-Art Cryptography" is being defined for the harmonised standards.

5.2 A Single Source of Truth

Presently, the European Commission supports an *allow list* policy in selecting cryptographic mechanisms that are considered secure in CRA vertical standards. Under this policy, use of a cryptography mechanism that is not explicitly allowed by the harmonised standards requires a third-party assessment (or some explicitly defined mitigation). Furthermore, rather than having all of the vertical standards contain their own lists and recommendations, a central, frequently updated "single source of truth" on allowed cryptography is preferred.

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:

- There is a need to access (decrypt) legacy encrypted information, and to verify its authenticity and integrity using legacy mechanisms.

[**] EC Std. request dated 03.02.2025, C(2025) 618, Annex II, Objectives. `https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)618&lang=en`

– Devices must be able to communicate and interoperate with older devices and with devices in other regulatory frameworks.
– There must be a way to introduce new cryptographic mechanisms into use without the need to insert them into ACM listings first.

A guiding principle for the application of the *allow list* is the “secure defaults” requirement (ECR P1-2-b) – the *allow list* defines what those defaults can be, but a user may reconfigure a product to use other mechanisms. Furthermore, in the case of a protocol negotiation, the product should opt for a mechanism in the *allow list* by default.

We observe that while CRA requires, e.g., automated updates, it also mandates that a user must have a way to postpone or opt out of them (ECR P1-2-c). Consumer devices are always ultimately under the control of their owners.

5.3 ACM and the Need for Public Consultation

Cryptographic algorithms supported in CRA will need to be compatible with other European regulations and policies, as well as the requirements of the individual national cybersecurity certification authorities (NCCAs).

With the 2019 EU Cybersecurity Act updates[††], many elements of the long-running SOG-IS (Senior Officials Group - Information Systems Security) were adopted under ENISA and the European Cybersecurity Certification Group (ECCG)[‡‡], including the widely-cited document “Agreed Cryptographic Mechanisms” (ACM) [7]. This document is already used for EUCC (Critical products).

As stated in ECCG’s ACM document itself: *“Its purpose is to specify which cryptographic mechanisms are recognised agreed, i.e., ready to be accepted by all national cybersecurity certification authorities (NCCAs).”* Hence, the ACM listing can be seen as a least-common-denominator set that is acceptable to all NCCAs. As the CRA is an European regulation, and products placed on the market in any single country can be sold in any other European country, the definition of pre-approved cryptographic mechanisms seems to be most logically placed under ECCG.

The ECCG is relatively new, and based on our observations, the process for selecting cryptographic mechanisms for ACM appears to be mostly closed. It seems uncontroversial to suggest that the selection process would benefit from a more direct involvement of the open cryptography research community – the same community of cryptanalysts and cryptography engineering experts who have designed most of the recommended algorithms on the ACM list. Hence, we hope that a broader public consultation will be established for the purpose of maintaining the “allow list” for CRA. This could also make the process more forward-looking and responsive to emerging threats and technology demands.

[††] Regulation (EU) 2019/881 of 17 April 2019 (Cybersecurity Act) `https://eur-lex.europa.eu/eli/reg/2019/881/oj`

[‡‡] European Cybersecurity Certification Group (ECCG): `https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group`

5.4 What is in the ACM Right Now and What is Missing?

All cryptographic mechanisms listed in ACM v2.0 [7] are considered suitable for use, but they are divided into two classes:

- **Recommended mechanisms**: Considered practical state-of-the-art and have a security level of at least 125 bits.
- **Legacy mechanisms**: Acceptable, with a security level of at least 100 bits. Legacy mechanisms have a specified depreciation/sunset date after which they will be removed from the list.

The set of algorithms in ACM is presently quite limited, but it is (for the most part) a superset of algorithms approved by the U.S. NIST. The expectation is that the list will need to be expanded to accommodate the broader range of products under CRA.

- **Symmetric**: AES, 3DES (legacy – 2027), SHA2-256+, SHA3, MAC modes (including HMAC-SHA-1 with depreciation date 2030), Key derivation mechanisms, PBKDF2.
- **Asymmetric traditional**: RSA (key sizes under 3000 bits have a depreciation after 2025), DSA, DH, ECDH, ECDSA (many variants).
- **Asymmetric PQC**: ML-KEM, FrodoKEM, ML-DSA, SLH-DSA, XMSS, LMS. Generally, only PQC Category 3 ("192-bit") and above is allowed.

There are some obvious gaps: The ACM list includes TLS 1.2 and 1.3 (with specific ciphersuites), but currently does not mention IPSec or SSH protocols, commonly used for VPN and remote administration.

The ACM also includes brief discussions about person authentication, but this seems to be written for Common Criteria use cases only, such as Hardware Security Modules (HSMs). It is likely that vertical standards (such as those related to "smart home" and wearable devices) will require this to be substantially expanded.

5.5 Impact of Risk Environment: Implementation Testing

In quantitative risk analysis, after a certain threshold (currently the 125-bit minimum strength of ACM-recommended algorithms), cryptographic key lengths and other parameter settings do not significantly affect the risk of cryptanalytic compromise. However, implementation quality always has a non-negligible impact on exploitation risk – for example, via simple logical vulnerabilities from implementation bugs, or through a lack of countermeasures against side-channel attacks and fault injection attacks in more advanced cases.

Current proposal maps CRA product categories (Section 3.1) to implementation testing regimes as follows:

- **Default:** Vendors who have not implemented their own cryptographic libraries but use standard ones can refer to their documentation. Products with bespoke cryptography are elevated to the Important class.

– **Important Class I and II:** Functional testing based on test vectors (either self-certification or with a notified body).
– **Critical:** European Cybersecurity Certification Scheme at "high" assurance level (AVA_VAN.3 or higher in case of EUCC [11]).

Note that U.S. FIPS 140-3 [20,21] testing mostly remains limited to functional testing. Plans are underway to establish a test vector service similar to NIST's CAVP (Cryptographic Algorithm Validation Program) under ECCG.

5.6 Cryptographic Agility ?

One further factor presently affecting the selection of algorithms is the transition to Post-Quantum Cryptography. While the current 2.0 (April 2025) version of the ACM [7] document includes warnings about quantum threat, it does not (yet) specify concrete sunset dates for traditional algorithms.

Previously, various European nations have offered their own guidance on this matter, but in June 2025, EU member states issued a "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography" [12]. CRA is discussed in the PQC Roadmap with the expectation of incorporating its transition requirements. Since it is expected that ACM will incorporate the sunset dates of the PQC Roadmap, it can indirectly serve as an enforcement mechanism for the European PQC transition in the context of CRA.

Table 2 summarizes the proposed transition timelines in the initial version of the European PQC roadmap. We note that the transition dates are mostly compatible with those proposed in the United States by NIST [16]. The timelines (as well as the algorithm selection) of CNSA 2.0 [5] seem stricter, but the scope of CNSA 2.0 is limited to U.S. National Security Systems (NSS – Defence and Intelligence Community systems).

When examining PQC transition guidance, it is useful to note that CRA is product legislation. CRA does not concern organisations that merely use products with cryptographic features; the CRA standards directly impose requirements on vendors and manufacturers that make the products. The approach in EU Coordinated Roadmap [12] and its referenced risk-analysis methodology [1] is largely organisation-oriented; there is a suggestion to "include supply chain" and to start the dialogue with product and service suppliers because the transition depends on them (in *first steps*) and to include cryptographic agility in procurement and NIS2 conformity (in *next steps*). The NIST White Paper on Cryptographic Agility [2] is also largely organisation-centric, but includes some technical and product-oriented guidance as well.

As cryptographic transitions are a continuous process, and unlikely to be limited to the current modernization process related to PQC, CRA may adopt more abstract design requirements loosely derived from a cryptographic agility definition given in [15]:

1. products should 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

Table 2. The Initial European PQC Transition timetable, reproduced from Section 4.1 of [12], dated June 2025. We refer the reader to that document for more detailed information about First Steps and Next Steps, and the risk levels used.

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.

2. products should have the ability to add new cryptographic mechanisms to existing hardware or software, resulting in new, stronger security features
3. products should have the ability to gracefully retire cryptographic mechanisms that have become either vulnerable or obsolete

For testable product requirements related to cryptographic agility, we note that the CRA [13] discusses product support periods in detail, as well as the mechanisms for dealing with artificially short ones. Generally, this is expected to be at least 5 years; especially for hardware products, it can be significantly longer.

One proposal is to require demonstrable cryptographic agility (to some alternative scheme, not necessarily the final replacement scheme used) if the product has a legacy cryptography mechanism (as defined in ACM [7]) as a default, and the announced depreciation of that cryptographic mechanism occurs during the product's support period.

6 Conclusions

This work examines the current state of development of European product standards related to the EU Cyber Resilience Act (CRA), with a focus on their impact on cryptography. CRA may have a positive effect, particularly by facilitating the transition to more robust algorithms and accelerating the Post-Quantum transition in internet-connected consumer electronics.

The cryptographic definitions in the closely related Radio Equipment Act (RED) standard series EN 18031 can be considered unsatisfactory (Section 4), and we hope that CRA will bring improvement to this by requiring strong cryptography as a default setting in products (users must still be able to use arbitrary cryptographic mechanisms). This work discusses the possible organisation of the cryptography approvals with ECCG (European Cybersecurity Certification Group) as the "single source of truth", and the impact of the Post-Quantum Cryptography transition on product requirements expressed in the standards.

Based on our experience with CEN and CENELEC, we offer criticism of their closed standardisation processes. To work on these standards (or even to find out about their direction), the author had to be appointed to CEN and CENELEC by two national-level Finnish standardisation committees (which mostly work as industrial associations). This path is not even feasible for citizens of some other EU countries. Furthermore, a member of a specific committee is generally not allowed to share working documents, even with members of other CRA standardisation committees, let alone with outsiders such as independent security researchers.

In addition to the fundamental problems of inaccessibility of technical information leading to low-impact standards, a closed standardisation approach is especially dangerous when applied to regulation related to cryptography and information security, where deliberate backdoors are a distinct risk in addition to simpler security issues stemming from a lack of an open, critical review by outside experts.

References

1. Amadori, A., Attema, T., Bombar, M., Duarte, J.D., Dunning, V., Etinski, S., van Gent, D., Lequesne, M., van der Schoot, W., Stevens, M., AIVD Cryptologists: The PQC Migration Handbook, revised and extended 2nd edition (December 2025), https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf
2. Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, W., Housley, R., Turner, S., Barker, W., Scarfone, K.: Considerations for achieving crypto agility – strategies and practices, second public draft. NIST Cybersecurity White Paper NIST CSWP 39 2pd, National Institute of Standards and Technology (July 2025). https://doi.org/10.6028/NIST.CSWP.39.2pd
3. Bernstein, D.J., Lange, T., Niederhagen, R.: Dual EC: A standardized back door. In: Ryan, P.Y.A., Naccache, D., Quisquater, J. (eds.) The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday. Lecture Notes in Computer Science, vol. 9100, pp. 256–281. Springer (2016). https://doi.org/10.1007/978-3-662-49301-4_17, https://eprint.iacr.org/2015/767
4. Caraco, J., Géraud-Stewart, R., Naccache, D.: Kerckhoffs' legacy (2020), https://eprint.iacr.org/2020/556

5. CNSS: Use of public standards for secure information sharing. CNSSP 15 – Committee on National Security Systems (CNSS) Policy No. 15 (December 2024), https://www.cnss.gov/CNSS/issuances/Policies.cfm
6. Davis, H., Green, M.D., Heninger, N., Ryan, K., Suhl, A.: On the possibility of a backdoor in the Micali-Schnorr generator. In: Tang, Q., Teague, V. (eds.) Public-Key Cryptography - PKC 2024 - 27th IACR International Conference on Practice and Theory of Public-Key Cryptography, Sydney, NSW, Australia, April 15-17, 2024, Proceedings, Part I. Lecture Notes in Computer Science, vol. 14601, pp. 352–386. Springer (2024). https://doi.org/10.1007/978-3-031-57718-5_12, https://eprint.iacr.org/2023/440
7. ECCG: Agreed cryptographic mechanisms. European Cybersecurity Certification Group Sub-group on Cryptography, Version 2.0 (April 2025), https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
8. ETSI: CYBER; cyber security for consumer internet of things: Baseline requirements. European Standard ETSI/EN 303 645 V3.1.3, European Telecommunications Standards Institute (September 2024), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
9. ETSI: Cyber security (CYBER); cyber security for consumer internet of things: Conformance assessment of baseline requirements. Technical Specification ETSI TS 103 701 V2.1.1, European Telecommunications Standards Institute (May 2025), https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/02.01.01_60/ts_103701v020101p.pdf
10. European Commission: The 'blue guide' on the implementation of EU product rules 2022. Official Journal of the European Union (2022/C 247/01) (June 2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC
11. European Commission: EUCC. Official Journal of the European Union (2024/482) (February 2024), https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj
12. European Commission: A coordinated implementation roadmap for the transition to post-quantum cryptography. Part 1, Version: 1.1, EU PQC Workstream (June 2025), https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
13. European Parliament: Cyber Resilience Act. Official Journal of the European Union (2024/2847) (November 2024), https://eur-lex.europa.eu/eli/reg/2024/2847/oj
14. ISO: Information technology– security techniques – random bit generation. Standard ISO/IEC 18031:2011, International Organization for Standardization (2011), https://www.iso.org/standard/54945.html
15. McKay, K.: How the national institute of standards and technology thinks about cryptography. In: Johnson, A.F., Millett, L.I. (eds.) Cryptographic Agility and Interoperablity – Proceedings of a Workshop. pp. 19–23. The National Academies Press (2017). https://doi.org/10.17226/24636, https://nap.nationalacademies.org/24636
16. Moody, D., Perlner, R., Regenscheid, A., Robinson, A., Cooper, D.: Transition to post-quantum cryptography standards. Internal Report NISTIR 8547 ipd, National Institute of Standards and Technology (November 2024). https://doi.org/10.6028/NIST.IR.8547.ipd
17. NEN: Common security requirements for radio equipment - part 1: Internet connected radio equipment. Standard NEN-EN 18031-1:2024, Nederlands Normalisatie Instituut (2024), https://connect.nen.nl/Standard/Detail?name=NEN-EN+18031-1%3A2024+en

18. NEN: Common security requirements for radio equipment - part 2: radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment. Standard NEN-EN 18031-2:2024, Nederlands Normalisatie Instituut (2024), https://connect.nen.nl/Standard/Detail?name=NEN-EN+18031-2%3A2024+en
19. NEN: Common security requirements for radio equipment - part 3: Internet connected radio equipment processing virtual money or monetary value. Standard NEN-EN 18031-3:2024, Nederlands Normalisatie Instituut (2024), https://connect.nen.nl/Standard/Detail?name=NEN-EN+18031-3%3A2024+en
20. NIST: Security requirements for cryptographic modules. Federal Information Processing Standards Publication FIPS 140-3 (March 2019). https://doi.org/10.6028/NIST.FIPS.140-3
21. NIST, CCCS: Implementation guidance for FIPS 140-3 and the cryptographic module validation program. CMVP (September 2025), https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
22. Stevens, M., Bursztein, E., Karpman, P., Albertini, A., Markov, Y.: The first collision for full SHA-1. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I. Lecture Notes in Computer Science, vol. 10401, pp. 570–596. Springer (2017). https://doi.org/10.1007/978-3-319-63688-7_19
23. Trummová, I., Schmüser, J., Huaman, N., Fahl, S.: Competing for attention: An interview study with participants of cryptography competitions. In: Proceedings of 32nd ACM Conference on Computer and Communications Security (CCS '25). p. to appear. ACM (2025)
24. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3621, pp. 17–36. Springer (2005). https://doi.org/10.1007/11535218_2