European Semiconductor Industry Association

POSITION PAPER

Key recommendations for the implementation of the EU Cyber Resilience Act

Brussels, 18 April 2025

Executive Summary

Semiconductors are key components of everyday electronic devices that make life easier, safer, more secure, and greener. From ground and air transportation to passports, payment cards, terminals, servers in data centres, desktop computers, sensors, etc., semiconductors are ubiquitous, fulfilling a crucial role in the whole domain of the Cyber Resilience Act (CRA).

In the opinion of ESIA members participating in the CRA implementation activities, there is a need to prevent for a disconnect to arise between the intentions of the European Commission and the reality of the semiconductor industry. Two key aspects need to be addressed. First, while industry best practices clearly distinguish between a semiconductor as a product / component with digital elements and the electronic product in which said semiconductor is incorporated, the European Commission does not seem to make this differentiation, as reflected in the proposed CRA legal text. Second, according to the existing industry best practices a given form factor does not determine the level of criticality of the product. However, the European Commission seems to use an interpretation that does not correspond to industry best practices and contradicts the CRA's risk-based approach and principle of proportionality.

ESIA is concerned that the above discrepancy may negatively impact the implementation of the CRA and believes an alignment is critical. For the sake of a smooth CRA implementation, ESIA calls on the European Commission to ensure – through a clarification in the Implementing Regulation of the CRA – that the existing best practices in the semiconductor industry are used.

Rue de la Duchesse 11/13
1150 Brussels
Belgium

Tel.: +32 2 290 36 60
Fax: +32 2 290 36 65
secretariat@eusemiconductors.eu
www.eusemiconductors.eu

ESIA is an industry association under the umbrella of
EECA: European Electronic Component Manufacturers' Association
EU Transparency Registry: 22092908193-23

Introduction

The CRA published in the European Official Journal on 20 November 2024 is an important legislation that drives Europe towards a safe and resilient digital landscape. This future will enable individuals, industries, and society to thrive with digital products and services while minimising the risk of both intended and unintended cyber incidents. An objective that requires transparency, where users have visibility of the inherent risk of the products with digital elements they acquire.

The European Semiconductor Industry Association (ESIA), representing the semiconductor industry and research in Europe, supports executing effective, scalable, and commercially viable ways to reach the CRA objectives of building a cyber resilience market. Drawing from years of experience in the security semiconductors domain, ESIA members have expertise in applying their security knowledge and skills to every market and application.

As we embark on a new phase of the CRA with its entry into force and upcoming Implementing Regulation, ESIA would like to request the European Commission to ensure – through clarification in the Implementing Regulations of the CRA – that the semiconductor industry's best practices are followed, in particular with regard to the differentiation between semiconductors and final electronic products.

I. Consider the proportionality to the risk

A given form factor (e.g., a smart card) should not determine the level of criticality of the product with digital elements. ESIA strongly encourages the European Commission, and its services involved in standardisation efforts as well as in drafting the Implementing Regulation as described in Article 7(4) of the CRA, to consider the proportionality to the risk and in particular the following elements and arguments:

- Semiconductor security implementation varies in nature and robustness, as semiconductors are the core of the operation for any product with digital elements. From cost, performance, use case, and risk perspectives, this variation allows Original Equipment Manufacturers (OEMs) – the customers to semiconductor companies – to select the right fit for the purpose.
- It is important to distinguish and differentiate between semiconductors as a product with digital elements and the electronic devices in which the semiconductors are incorporated. For example, a product with a form factor of a smart card cannot and will not be of the same nature as a *secure element* in terms of functionality and criticality, but both products rely on a similar platform based on semiconductors. A risk analysis should be carried out to identify relevant and applicable requirements to a given product with *secure elements*.
- The common denominator of all "*smart cards and similar devices*", including *secure element* is the high tamper-resistant hardware which may or may not

include the firmware / operating system. This high *tamper resistance* is the unique characteristic of a *secure element*, which differentiates it from other semiconductor products. The industry follows the definition created by SOG-IS for "*smart cards and similar devices*" and its respective technical domain, and from which CRA borrowed the term. This high tamper-resistant hardware is a "*smart card and similar devices*" product in its own right and the most important one. Changing this widely accepted industry definition by introducing a different CRA definition would result in the opposite objective intended by the CRA of transparency and resilience for products used in critical applications, and hence in the Critical CRA Class.

- To use an analogy: Having wheels is a good parameter to identify vehicles. However, there are vehicles with two, three, four, or more wheels. They belong to different classes, and they are treated accordingly. Applying this principle to the taxonomy definition shows the importance to differentiate the *tamper resistant* for Class II products and the *tamper resistant* applicable to "*Smartcards or similar devices, including secure elements*"[1] for a proper CRA implementation. If the mere fact of having wheels makes a product an automobile, that calls for confusion. If the mere fact of having *tamper resistance* makes a product Class II, that calls for confusion. **If the smart card form factor is the only criterion that makes a product a Critical Product, that calls for confusion.**
- Equally, not all products which happen to appear in the form of a "*plastic card*" qualify as "*smart cards*". The reason is that it is not the form and the plastic around it that qualify a product as a "*smart card*", but the high *tamper resistant* microcontroller (MCU) which is inside. In that sense, access cards to a gym or a ski-lift cannot be considered as smart cards. This very same rationale is the reason why a *product with digital elements* utilising a component from the Critical Class, like *secure elements*, does not become part of the Critical Class by the mere fact of using that *secure element* component.

[1] Annex IV(3), of Regulation (EU) 2024/2847 (Cyber Resilience Act). Source: OJ L, 2024/2847, 20.11.2024, p. 72.

II. The cornerstone of the CRA is the risk-based approach

According to the CRA[2], certain product types might require stricter conformity assessments, keeping a proportionate approach. The selection of the conformity assessment based on the class type is relative to the negative impact of cyber incidents on products with digital elements. The product classifications are dependent on core product functionalities. Critical products are those that carry a significant risk of adverse effects in terms of their intensity and ability to disrupt, control, or cause damage to a large number of other *products with digital elements* through direct manipulation. Modules for conformity assessment procedures are established, in proportion to the level of risk involved and the level of security required.

The below paragraphs provide more details and additional arguments:

1) The core product functionality is the driver for classification

- For example, in Annex IV(3)[3], a *secure element*, and smart card, from a functional approach in the semiconductor industry, implies the same functionality in terms of security functionality and high tamper resistance. However, for an audience who is not familiar with those terms, or security expertise, the CRA does not sufficiently distinguish between the two.
- A "*plastic*" smart card form factor product, like for example an access control card, might use a *secure element* as its core. The smart card form factor product used for access control cannot be deemed as a critical product just because it uses a smart card component like the *secure element*. It would be wrong to place it in the same category as a *secure element*, as the core functionality is different: access control vs. strong tamper resistance.
- Equally, an access control card might use a less tamper resistant MCU outside the *secure element* domain and definition, an MCU from Class II as tamper resistant, or even MCU from Class I without tamper resistance. It is a clear deviation from the CRA principles of functionality: while it looks the same as the card with a *secure element*, **it is not the same functionality**. Making it equivalent or comparable, having both in the Critical Class diminishes the whole purpose and whitewashes the meaning of Criticality of the products from a CRA perspective. Plus, if the MCU is from Class I, this might force manufacturers to perform third-party assessments, once more outside the CRA's intended applicability.

[2] Recitals (44), (45), (46), and (90) of Regulation (EU) 2024/2847 (Cyber Resilience Act). Source: OJ L, 2024/2847, 20.11.2024, p. 11, 20-21.
[3] OJ L, 2024/2847, 20.11.2024, p. 72.

2) There are different CRA classes for products with different impacts, requiring conformity assessment procedures in proportion to the level of risk involved and the necessary level of security.

- While the CRA does not require security levels, it sets a clear expectation to communicate the risk to users.
- This can only be possible if there is a metric to identify various security implementations, from a relative low risk level (e.g., consumer grade) to strong security (e.g., military grade). Rather than create or invent such metrics, the industry acknowledges and recommends existing metrics used within the semiconductor industry for grading security levels (for example AVA_VAN levels).
- The fact that tamper resistance is part of Class II MCUs and microprocessors (MPUs), as well as one key characteristic of *secure elements* in Annex IV(2)[4], calls for understanding that there are different levels of robustness or implementations across tamper resistance. Moreover, regulations like eIDAS[5] call for tamper resistance in the high level of assurance as physical tamper resistance at *secure element* grade, creating a precedent for such differentiation on implemented assurance levels.
- As this is not clearly identified in the CRA, it is strongly recommended that the Commission take it into consideration when drafting the applicable Delegated Acts, reflecting the market reality.

In the position paper published on 18 October 2024[6], ESIA followed the CRA legal text as guidance for drafting a proposal that, while at its core was intended to support the successful implementation of the CRA, also reflected the best practices in the semiconductor industry. While the CRA is a novelty in various sectors, the semiconductor industry is not new to the CRA risk-based approach and best practices: By the nature of the operation, semiconductors are used in or by any other product with digital elements.

[4] OJ L, 2024/2847, 20.11.2024, p. 72.
[5] Regulation (EU) No 910/2014. Source: OJ L 257, 28.8.2014, p. 73-114.
[6] "*Contribution to the definition of critical products under the CRA*" at https://www.eusemiconductors.eu/sites/default/files/20241018_ESIA-Position-Paper-CRA.pdf

III. A support period of equal duration across all products, for a predictable, well aligned framework

The CRA states that an Administrative Cooperation Group (ADCO)[7] made up of surveillance authorities, shall issue recommendations as referenced in Article 52(16)[8]. The Commission may adopt those recommendations as Delegated Acts[9] to enhance the CRA by specifying the minimum support period for product categories where the market surveillance data indicates inadequate support periods[10].

Recital (60)[11] calls for such considerations on products with digital elements that are reasonably expected to be used for longer than five years, as is often the case for hardware components such as motherboards or MPUs, and more where manufacturers are expected to act accordingly, ensuring longer support periods.

ESIA strongly recommends not to create any exceptions – i.e. no support periods longer than the standard five-year duration – for semiconductor products. Due to the nature of the semiconductor business, where customers are professional users (B2B), the duration of the support period is already clearly included in contractual obligations between semiconductor companies and their customers. An exceptional longer support period for semiconductors would create additional administrative burden to the industry with negative consequences on its competitiveness, without reasonable business justification.

Conclusion

As key components of everyday electronic devices and critical digital infrastructures and applications, semiconductors are indispensable to Europe's cyber resilience, industrial success, the green and digital transition, technological sovereignty, and economic security. Semiconductors are an industry of true strategic importance for Europe.

ESIA welcomes the CRA and calls on the European Commission to adopt an approach to cyber resilience – in the Implementing Regulation of the CRA – that reflects the existing best practices in the semiconductor industry, and accordingly differentiate between a semiconductor as a product / component with digital elements from the final electronic product in which said semiconductor is incorporated.

ESIA stands ready to cooperate with the European Commission to achieve this goal.

[7] The ADCO is established under Article 52(15). Source: OJ L, 2024/2847, 20.11.2024, p. 58.
[8] OJ L, 2024/2847, 20.11.2024, p. 58.
[9] Article 61 of Regulation (EU) 2024/2847 (Cyber Resilience Act). *Ibid.*, p. 63.
[10] Article 13(8) of Regulation (EU) 2024/2847 (Cyber Resilience Act). *Ibid.*, p. 36.
[11] OJ L, 2024/2847, 20.11.2024, p. 15.

For further information:

Giovanni Corder
European Semiconductor Industry Association (ESIA)
Tel: + 32 2 290 36 60 • Web: https://www.eusemiconductors.eu/

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the semiconductor industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies, the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as one of the most R&D-intensive sectors by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 jobs indirectly in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.