European Semiconductor Industry Association

POSITION PAPER

Contribution to the definition of critical products under the CRA

Brussels, 18 October 2024

Introduction

The European Semiconductor Industry Association (ESIA), representing Europe-based semiconductor designers, manufacturers, and research institutes, would like to bring to the attention of the European Commission its interest in participating in developing the definitions applicable to the semiconductor industry in the context of the Cyber Resilience Act (CRA).

The semiconductor industry is an Important Entity defined by the Network & Information Security 2 Directive (NIS 2)[1] given its importance in developing digital societies. The semiconductor industry in Europe is one of the most prolific and relevant globally for security-related applications. On top of it, other industries like electronic payments, eIDs, transportation, public key infrastructures (PKI), energy, space, industrial, etc., thrive in Europe supported by the semiconductor industry. Therefore, ESIA finds it extremely important to share facts and opinions about the fundamentals of this industry, and its applicability in the definition of the CRA Classes.

Europe-based semiconductor companies operate and sell in a global Smartcard microcontroller unit (MCU) market valued at US$ 4.3 billion in 2023. The market for microprocessor units (MPUs) amounted to over US$ 45 billion in 2023, while the market for application-specific integrated circuits (ASICs) surpassed US$ 248 billions[2].

[1] *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, OJ L 333, 27.12.2022, p. 80-152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (retrieved 18/10/2024)

[2] World Semiconductor Trade Statistics (WSTS), 2024

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

I. Industry Definitions

Intellectual Property (IP) Blocks

- Any Chip consists of one or more IP blocks. Each of those IP blocks performs specific tasks within the chip, like storage (memory), memory interfacing, cryptographic processing, memory encryption, central processing unit (CPU), graphics accelerator, artificial intelligence (AI) acceleration, or communication like Bluetooth Low energy (BLE), WiFi, Near Field Communication (NFC), Serial Peripheral Interface (SPI), Inter-Integrated Circuit (IIC or I^2C), Ethernet, Controller Area Network (CAN), etc.
- IP blocks can be placed on the market as Soft-IP (Very High Speed Integrated Circuit Hardware Description Language, or VHDL, code) or as Hard-Macros (pre-designed hardware modules).
- IP blocks can be acquired from third parties or be designed in-house by the silicon vendor.

User-Programmable Memory

- It is a memory whose content can be programmed by the party buying the chip.

Firmware

- Firmware is a software component which provides an interface to basic functionalities like cryptographic libraries, connectivity libraries, secure boot, etc.

Microprocessor Unit (MPU)

- An MPU is a chip that has a central processing unit and integrated volatile memory, but without ano non-volatile user-programmable memory for code. The application code is stored in an external memory outside of the MPU. MPUs might have limited non-volatile memory allowing to store limited data information.

  Note: The following are two prominent examples of MPU configurations that can be placed on the market:

  - As a chip: Hardware with a minimum code (or hardware logic) allowing software to boot.
  - As a chip in combination with firmware.
    - The firmware can be pre-installed with the chip or be delivered as part of the Software Development Kit (SDK) of the MPU.

Microcontroller Unit (MCU)

- An MCU is a chip that has a central processing unit and integrated volatile memory and non-volatile user-programmable memory to store application code and data.

  Note: The following are two prominent examples of MCU configurations that can be placed on the market:

  - As a chip: Hardware with a minimum code (or hardware logic) allowing software to boot.
  - As a chip in combination with firmware.
    - The firmware can be preinstalled with the chip or be delivered as part of the SDK of the MCU.

Application-Specific Integrated Circuits (ASIC)

- ASICs are tailored (micro)chips designed to perform application-specific tasks providing optimisation (like cost, processing speed, performance, etc.).
- ASICs have processing capability implemented in hardware logic with CPU and / or specialised gates.
- ASICs' programmability by the customer is not intended or even possible.

Field-Programmable Gate Arrays (FPGA)

- A Field-Programmable Gate Array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing.
- It contains an array of programmable logic blocks and a hierarchy of reconfigurable interconnects that allow the blocks to be wired together.
- FPGAs can be used to implement any logical function that an ASIC could perform, but with the advantage of post-manufacturing flexibility. They are widely used in applications requiring rapid prototyping, custom computing, and real-time processing.

Secure Platform for Smartcards and Similar Devices

- A Secure Platform is composed of a chip, firmware, and an optional Operating System (OS).
  - A chip with a central processing unit and volatile and non-volatile user-programmable memory to store application code and data, **providing high Tamper Resistance**.

- The Secure Platform can be placed in the market with two basic configurations:
    - As a chip in combination with firmware.
    - As a chip in combination with firmware and pre-installed OS.
- The product with digital elements in a CRA context is commercialised as **Secure Element**.

Smartcards and Similar Devices

- They are solutions by themselves.
- They run on high Tamper Resistance "*Secure Platform for Smartcards and similar devices*":
    - As composed by Applets, i.e. application(s) implementing the service(s), and the Secure Platform.
    - A specific business logic is implemented in software, for example as part of a dedicated OS running on a chip with firmware. It can be understood also as applications implemented in a monolithic way on the "*Secure Platform for Smartcards and similar devices*".
- They are available in various form factors:
    - The product with digital elements in a CRA context is commercialised as a **Secure Element** when it is an embedded component in a larger system. Typical examples are eSIMs, Trusted Platform Modules (TPMs), automotive Hardware Security Modules (HSMs), etc.
    - The product with digital elements in a CRA context is commercialised as a **Smartcard** when it is a stand-alone component. Typical form factors include banking cards, eID cards, access control cards, etc.
- The main characteristic of Smartcards and similar devices is their high Tamper Resistance.
- The underlying hardware layer, the "*Secure Platform for Smartcards and similar devices*", provides the high Tamper Resistance of the Smartcards and similar devices.

Hardware Devices with Security Boxes

- These devices rely on the security and Tamper Resistance characteristics of "*Smartcard and Secure Element*" for providing security functionality at the same, or equivalent tamper-resistance level.
- The use of "*Smartcard and Secure Element*" can be done in two ways:

- Integrated (embedded, soldered in the printed circuit board, etc.) in the "*box*", with an enclosure providing additional Ramper Resistance.
- As a discrete component that can be added / removed by end-users (customers or authorised operators).

- The industry adopted this definition for products whose security capabilities could be measured in the same technical domain as those from "*Smartcard and Secure Element*", using the same attack potentials, rankings, etc.

II. Technical Definitions

Logical Attacks

- **Logical attacks** rely on the device's interfaces to modify the intended behaviour of security functionalities (e.g., installation of new software, buffer overflow, weakness in communication protocols, etc.) or interfere with the software / firmware on the device.

Security Functionalities for FPGAs, ASICS, MCUs, MPUs, Secure Elements and Smartcards

- A **security functionality** of a device is a function which implements or supports the integrity, confidentiality, or authenticity of the user assets handled by the device, to be securely protected at minimum against logical (network and software) attacks.
- A security functionality follows a specification, and it has well-defined interfaces via which the user can use / invoke it.
- The security functionality includes functions like cryptographic operations, key generation, including (True) Random Number Generators (or (T)RNGs) when used for cryptography, as well as secure…
  - storage;
  - debugging;
  - boot;
  - isolation;
  - channel protocol;
  - updates; and
  - attestation operations.

Tampering Attacks

- The **tampering attacks** usually rely on exploitation, modification, or interference of the device's physical characteristics, aiming to modify the intended behaviour of security functionalities.

- These attacks require physical access to the device.
- There are three types of physical attacks:
    1. non-invasive (the device is not modified physically);
    2. semi-invasive (which require to physically modify the chip without destroying it and it can still function); and
    3. invasive attacks (the chip is more heavily physically modified and eventually destroyed).

Joint Interpretation Library (JIL)

- The Joint Interpretation Library (JIL) is a group of experts from the industry and national cybersecurity authorities in Europe.
- JIL uses a point system of international recognition for identifying attacks and assigning points that allow security experts to qualify product security robustness.
- Its main focus is hardware attacks.
- This point system is used in several certification schemes, Common Criteria (EUCC) for example, providing a first line of harmonisation as per what is in, and what is out when describing the security resistance of a product against different attacks.
- The JIL point system clusters the resistance of the products in categories as 'basic', 'enhanced basic', 'moderate', and 'high'.

Tamper Resistance

- The **Tamper Resistance** of a device is defined as the effectiveness of the protection of the product's security functionality against tampering attacks.
- The hardware provides the product's Tamper Resistance.
- Tamper Resistance is a property of a security functionality.

High Tamper Resistance

- **High Tamper Resistance** of a device is provided by the security's functionality protection against the most sophisticated and complex tampering attacks in the JIL scale attacks, typically expressed as 'moderate' or 'high' attack resistance.

CRA Product Classes

CRA Class 0 Products, or default category: Products without security-related functionalities

- The lack of those "*security-related functionalities*" implies that from a risk-based approach, the manufacturer informs the users that those products are not suitable for applications directly exposed to threats, or those applications need to be hardened by the users.
- Examples include MCUs for motor control subsystems controlled by a central control unit.

CRA Class I Products: MCUs and MPUs with security-related functionalities

- For most of the industry, when it comes to "*security-related functionalities*", both MCUs and MPUs are equivalent.
- "*Security-related functionalities*" imply one or more protections against logical attacks, including but not limited to the execution of unauthorised firmware / software, unauthorised memory access, unauthorised access to services, etc.
- While there are different implementations of such "*security-related functionalities*", matching various resistance levels, they tend to stay in the lower band of resistance. Typically, the 'basic', 'enhanced basic' attack potential in the JIL scale.
- The "*security-related functionalities*" can be hardened by implementing tamper-resistance capabilities.

CRA Class II Products: Tamper-resistant MCUs and MPUs

- For most of the industry, when it comes to "*tamper-resistant*", both MCUs and MPUs are equivalent.
- "*Tamper-resistant*" implies resistance against non-, semi- and invasive attacks. However, the invasive attacks are reserved for the high-end security of ***"Smartcards or similar devices, including secure elements"*** in the CRA Critical Products category.
- For that reason, two criteria apply:
    - Tamper Resistance is one or more protections against non-invasive and semi-invasive attacks:
        - Non-invasive attacks: voltage / clock glitch, electromagnetic fault injection (EMFI), side channel attacks, such as timing or power (simple power analysis, SPA, or differential power analysis, DPA) and electromagnetic emission analysis.

        - Semi-invasive attacks: laser fault injection (LFI), optical emission analysis, induced leakage.
    - Tamper Resistance following the industry-established standards at JIL rating 'enhanced basic'.

CRA Critical Products: Smartcards or similar devices, including secure elements

- The CRA addresses Critical Products as products having a very important cyber impact, or large adverse effect in case of a security incident. For example, when the Secure Platform for Smartcards and similar devices hardware is compromised, it has a major impact on Smartcards or similar devices, users and applications.
- The terms Smartcard and Secure Element are used indistinctively by the industry with two meanings. Sometimes they refer to the product with high tamper resistant technology, the Secure Platform and sometimes to the entire solution, including the application.
    - As a **Secure Platform**, this technology is the most hardened tamper-resistant one, with the Tamper Resistance originating in the chip.
    - The technology supports critical applications where the Tamper Resistance of the chip protects information, or assets, from the most sophisticated attackers. Those with enough incentive, and means, to attempt breaking into those devices.
    - Security evaluation of **Secure Platform** for Smartcard products is usually done in Senior Officials Group Information Systems Security (SOG-IS) Common Criteria or in EUCC (after 2026).
        - Given the critical use of the technology, it is common best practice to evaluate and certify with Common Criteria to the highest levels for **Tamper Resistance**, usually vulnerability analysis AVA_VAN.4 or Evaluation Assurance Level (EAL) 5, and above.
        - Such evaluations are done at high CC assurance levels and target stringent assessment criteria to verify that the secure platform has an attack resistance against high-end tampering attacks.
        - Security certifications of **Secure Platform** and Smartcard products are in most cases following the composition approach where, in the first step, the security and attack resistance of the Smartcard hardware, the chip, is evaluated and certified at the same or even higher level of attack resistance than the Smartcard end-product. This is because the Smartcard hardware is the critical component for the overall Tamper Resistance of the Smartcard product.

- The EUCC Implementing Act[3] acknowledges the importance of the hardware layer in the **Secure Platform** for the expected security of smartcards, prioritising this domain: "*The first technical domain is the 'Smart cards and similar devices' technical domain, where significant portions of the required security functionality depend on specific, tailored and often separable hardware elements(e.g. smart card hardware, integrated circuits, smart card composite products, Trusted Platform Modules as used in Trusted Computing, or digital tachograph cards)*".

- Following the state-of-the-art document from European Union Agency for Cybersecurity (ENISA) for the EUCC, as applicable for the Cybersecurity Act (CSA)[4] 'high level', it is in the domain of AVA_VAN.4 or EAL 5, and above. The Tamper Resistance measurement follows the guidance from JIL at **Moderate** and **High** attack potentials.
- eIDAS refers to this technology as "*tamper resistant*" (eIDAS Article 8[5]).
- This technology is available to the market as a product from the semiconductor industry.
- The silicon industry refers to this kind of product as "*Secure Element*".
- As a **Secure Platform**, the product is delivered to the market in one of two basic configurations:
  - the chip with the necessary software to operate it (libraries, Application Programming Interfaces, or APIs, etc.); or
  - chip plus an OS.
- For either configuration, the hardware is certified under CC following the guidance expressed at the beginning of this section for **Tamper Resistance**.
  - When the Product consists of the hardware only, the user of the technology takes ownership of the integration and certification of the newly created platform as a product of their own.
- The **technology** can be used as a stand-alone application product once an application (Applet) is loaded onto the silicon platform.

[3] *COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)*, OJ L, 2024/482, 7.2.2024. URL: https://eur-lex.europa.eu/eli/reg_impl/2024/482/oj (retrieved 18/10/2024)

[4] *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, OJ L 151, 7.6.2019, p. 15-69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (retrieved 18/10/2024)

[5] *REGULATION (EU) NO 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, OJ L 257, 28.8.2014, p. 88-89. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj (retrieved 18/10/2024)

- While some semiconductor vendors might sell the technology with pre-loaded applications, as solutions, most of the business operations imply silicon vendors selling the technology. Third parties (users) upload their Applets and provide additional services supporting their product.

- The **applications** of this technology are seen in a wide number of use cases. From entry-level applications like physical access control to eID documents like passports.
    - Depending on the application and additional integration with other functionality, the name can be linked to the application, like for example "*Payment Card*", "*SIM*", "*eSIM*", "*Transport Card*", "*TPM*", "*HSM*", "*Physical Access Control Cards*", etc.
    - When the platform, the hardware, and the OS are designed for a dedicated application, even if the hardware is certified under CC following the guidance expressed at the beginning of this section for **Tamper Resistance**, the OS is treated as part of the application and evaluated under the rules of application to the specific risk level.
    - The verification of the proper integration of the technology, the security of the Applet and the entire solution as a product is evaluated per application.
        - Most of the applications targeting highly critical applications follow CC, or some optimised version of CC executed as a private scheme relevant to such industry. Examples include the GSMA eSA scheme, EMVCo, MIFARE, etc.

III. Recommendations

The semiconductor industry has been playing a very active role in securing products with digital elements in security-critical applications for many years. This experience has driven definitions, technologies, ranking systems, and market guidance for identifying and measuring security claims. The same experience is now applicable to semiconductor products outside security-critical applications. The CRA's adoption, and successful market implementation, is a natural evolution of the industry's experience.

This experience is the source of knowledge of the points referred to in this document:

- "*Smartcard and Secure Element*", as semiconductor products, are part of the Critical Products category per the CRA proposal. They have Tamper Resistance capabilities from 'moderate' and up to 'high' attack potential within the JIL ranking or equivalent.
- Secure Elements and Smartcards, as products with an application or Applet, as a product solution, will respond to market needs in different verticals, with different applications at different risk levels. While some of those applications will be looking at the same or similar Tamper Resistance from "*Smartcard and Secure Element*", not all of them will be at the same risk level. Hence, even if they are listed in the Critical Product category from Annex III in the CRA, the standards applicable to them need to reflect this reality. Moreover, through CRA Article 24 (3a)(b), the Implementation Acts should address the conformance of those outside the highly-critical domain as Class II conformance.
- From a security perspective, there is no need to further elaborate on the differences between MPUs and MCUs, as they can be treated simultaneously for conformance purposes.

Since "*Secure Platforms for Smartcards and similar devices*" are just one instantiation of semiconductors with the highest Tamper Resistance, to differentiate from products in Class II, a ranking system like JIL, AVA_VAN from CC or equivalent should be used as this Tamper Resistance is the key differentiator between these product classes.

- MCUs / MPUs without any Tamper Resistance claims, oriented to protect against logical attacks such as software and network versions, belong to Class I.
- Those principles of (high) Tamper Resistance and logical attacks, should be considered for any similar product as is the case of graphics processing units (GPUs), neural processing units (NPUs), complex Systems-on-a-Chip (SoCs) and many other variants of MCUs and MPUs. It will be confusing for the market products going into the default category because they are sold with other (application-related) names.
- A similar principle could be applied to products like ASICs and FPGAs.
- To prevent confusion in the market, a Product with digital elements belongs to one and only one CRA class and product category.

- The intended purpose should rule over the applicability of the product classes and conformance mechanism, as part of the manufacturer's claims on the product's security claims when placing the product into the market.
- Modularity, or Composition, is and has been for a long time a best practice in the security industry. This best practice will continue to be used under certification schemes like EUCC and for applications like eIDs and others in the highly secure domain. The industry expects Implementation Acts, and Standardization Requests, to issue recommendations for the use of Modularity, or Composition, as a mechanism to show conformance with the CRA. This will lower entry barriers for manufacturers, reduce conformance complexity and enable a successful CRA implementation.
- There is an imminent need to create awareness and educate the market. There is a limited number of specialists involved in the CRA developments. It's strongly recommended that this activity receives additional attention creating trainings, webinars, FAQs and other outreach mechanisms for reaching out to the market with the fundamental level of understanding of what CRA implies for all the players of the value chain of Products with Digital Elements.
- In addition to the previous points, we strongly encourage the Commission to elaborate cross-regulatory guidance addressing the different conformance aspects for NIS2, DORA, eIDAS, CSA, EUCC, RED, etc. and CRA, including reporting obligations and vulnerability management. This effort should be extended to other regulations where the evidence of proper cybersecurity implementation is applied like the liability act, safety act, machinery directive, etc.

While the road ahead is long, and there is much work to do, the industry strongly supports the successful implementation of the CRA. ESIA is willing to contribute through the different forums and channels with the Commission with expertise, and active contribution to those various activities.

IV. Afterword / Semiconductors contribution to the CRA implementation

The CRA will change the way that many verticals address security. By introducing best practices and the concept of security by design, users can make informed decisions with the information provided by the manufacturers. Helping them to identify, quantify and qualify the inherent risk of any product with digital elements.

There will be verticals where this will be a game changer. A true innovation. However, for products used in high-impact applications, like secure tamper resistant MCUs in payment and eID applications, which are high-risk, or MPUs used in millions of consumer PCs, such practices are known to the industry. The CRA provides an opportunity for the semiconductor industry to bring the industry's expertise to a wider audience of users and product manufacturers. Enabling them to address their conformance needs.

For example, an EV Charger unit in the CRA default category requires a self-declaration of conformance to the Essential Requirements. The manufacturer will need to make claims regarding its cryptography for protecting 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. Cryptography is a functionality supported directly by the semiconductors. This might be the case as well for key management, firmware authentication and other security mechanisms provided by the semiconductor for secure updates addressing vulnerabilities in the field. Hence, the EV Charger maker might address the semiconductor as a “module” for their declaration of conformance, referencing “module” conformance claims supporting the conformance claims of the charger manufacturer.

The information provided by the semiconductor manufacturer, beyond the description of the security capabilities of the chip and its strength or robustness, includes the guidance documentation, as per the CRA. This is a key component for users of those chips. It allows them to understand the risks involved in the (inadequate) use of the semiconductors and the activities that the user needs to implement for an effective use of the security capabilities of the chip.

The use of Semiconductors from Critical Class, Class II (Tamper-resistant), Class I (with security features), and default category (without security capabilities) follow the same principles: a risk-based approach for specific intended uses. The right fit for purpose.

For example, a microcontroller used behind a (very) heavy turbine inside a closed facility with limited and controlled access might only require protection against logical or remote attacks. “Tamper-resistance” might not be required for this use case. Even the mitigation countermeasures against logical or remote attacks will vary depending on the logical protection of the entire system, like network segmentation, firewalls, etc. A similar argument can be made for semiconductors without security capabilities. For example, an MCU controlling a step motor in an industrial robot arm when this MCU is controlled by an internal bus without (or with limited) physical access (e.g. dangerous waste disposal), isolated by a central unit segregating the internal bus from any external connections and other external network protections, etc. The central unit and the overall robot arm provide the "secure environment" allowing the MCU without security capabilities to operate securely. A developer might select MCUs without security capabilities in the same way a system integrator might select MCUs without Tamper Resistance to be used in a system where the environment provides the necessary security controls based on the risk analysis.

Even post-CRA, not every MCU/MPU needs cybersecurity as with any product with digital elements the development and use of products with digital elements is always a risk-based exercise in the context of the intend of use for that particular product.

For further information:

Giovanni Corder
Acting Director-General
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 sector by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs 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.