EUROSMART
The Voice of the Digital Security Industry

Eurosmart's position paper on CRA and modularity

Introduction

With the Cyber Resilience Act (CRA), Europe is making important steps towards building a cyber-resilient digital society. With the global trend of digitalization, the multiple benefits derived from it, and the exponential growth of digital applications, for facing the future implementing the CRA is the right thing to do.

The CRA fills a gap in the regulatory compliance space by complementing the manufacturers' obligations on safety, which is already well-established, with the introduction of security measures.

The CRA brings several innovations:

- The definition of a *product with digital elements*.
- Manufacturer's decisions are made on a *risk-based* approach.
- Security by design principle that needs to be supported during the product's lifetime.
- Address security risks through the product's supply chain.

The CRA recognizes that any product is the product of the sum of various parts, or **components**, as indicated in Article 3(6). Components can introduce potential risks. Hence, a secure supply chain is key.

CRA compliance for each hardware and software component is paramount for managing the risk of final products placed in Consumer, Automotive, MedTech and Industrial markets. Components' composition creates a product, and its integration creates a system. CRA applies horizontal rules and security by design principles across the entire supply chain.

Following the same logic, it's understood and expected that manufacturers will make design decisions based on the risk, selecting the components with security capabilities and robustness matching the application's risk level. As per Annex II of the regulation, a CRA conforming component shall provide compliance information with the cybersecurity essential and document requirements from the regulation. Making the security features and compliance of final products depend on those of their components, and its integration (composition).

A common practice in the electronics industry[1] is the development of common platforms for product ranges. A single common product platform can be used in entry-level products, as well as in high-end ones. It drives costs down. It optimizes operation. It's a rather scalable way to address various market segments. At times, the platform comes in the form of a module to provide specific product functionality across several product types.

Modularity is a concept that refers to the design and organization of systems or software in separate, independent components or modules. These modules can function independently and interact with each other through well-defined interfaces. The end product inherits the security properties from those modules when properly integrated. The modularity concept is therefore applicable to individual components, and the combination of those components in the form of platforms or modules.

Modularity is acknowledged by other regulations within the NLF like the RED for EMC. Modularity is a key aspect of a secure supply chain and secure products. Several provisions of the CRA legal text hint at modularity, however a specific reference to modularity in the regulation and detailed approach are necessary for a correct applicability. This paper highlights the need to include modularity in the Implementation Acts and to develop guidance in the form of a horizontal standard, making modularity part of the toolkit for CRA conformance, and providing an efficient and scalable method for a successful CRA implementation.

Component's risk management in Products with Digital Elements

The CRA makes several assertions towards risk management:

- Propagation of risk is addressed in the CRA by the fact that "*The severity of the impact of an incident may also increase where the product performs a central system function, including network management, configuration control, virtualisation or processing of personal data*". A similar argument could be made about *the Security capabilities of a component performing a central system function that can be used as-it-is or be the foundation for other security functionality in the product where is integrated.* As a component can introduce risk, equally can be understood that a robust component can help mitigate the risk of the products where it is used. As a single component can be used across multiple products, the positive impact can be reflected on a larger scale.
- Every decision made by the manufacturer is risk-based. Selecting components is one of them. Selecting the right components when security is not a core expertise is hard. The CRA will provide a mark, the CE mark, to suppliers meeting the CRA conformance but it does not tell anything about the risk level, security functionality and usage of the component for helping manufacturers select the right fit for purpose. Manufacturers need the knowledge, to understand the security functionality, and strength of its implementation, of components for making design and acquisition decisions risk-based. Selecting the State-of-the-Art (SOTA) technology, the right component, suitable to the application risk level.
- Integration guidance is key information for the users of components: Making effective use of the security capabilities provided by the component while avoiding introducing

[1] Study on the need of Cybersecurity requirements for ICT products –No. 2020-0715
4.1.4. Stakeholders involved in the lifecycle
https://cdn.ceps.eu/wp-content/uploads/2022/01/VIGIE20200715_Cybersecurity-requirements-for-ICT-products.pdf

additional risks in the process. It makes sense that users have guidance on how to address conformance claims of their products when they rely on the conformance claims of the components.

CRA conformance: An exercise of aggregation (modularity)

Modularity is key for the successful implementation of the Cyber Resilience Act.

CRA treats in the same way end devices and components are placed on the EU market separately. The requirements and obligations of the end devices will be supported to some degree by the components.

Defining guidance for manufacturers and 3rd party product assessment organizations about how to use evidence of the security capabilities of components for claiming CRA conformance on end products is critical.

For manufacturers, it is particularly important for products in the default category (Figure 1):

- Products in the default category are subject to the same obligations and requirements as any other products.
- When the manufacturer makes an incorrect statement, independently of the reasons behind it, they are still subject to the same penalties as the rest of the products.
- Manufacturers might not be able to obtain the required information from their suppliers specific to the conformance claims in their products.
- With so many layers and components built into a product, even the use of SBOMs and similar tools falls short when addressing conformance

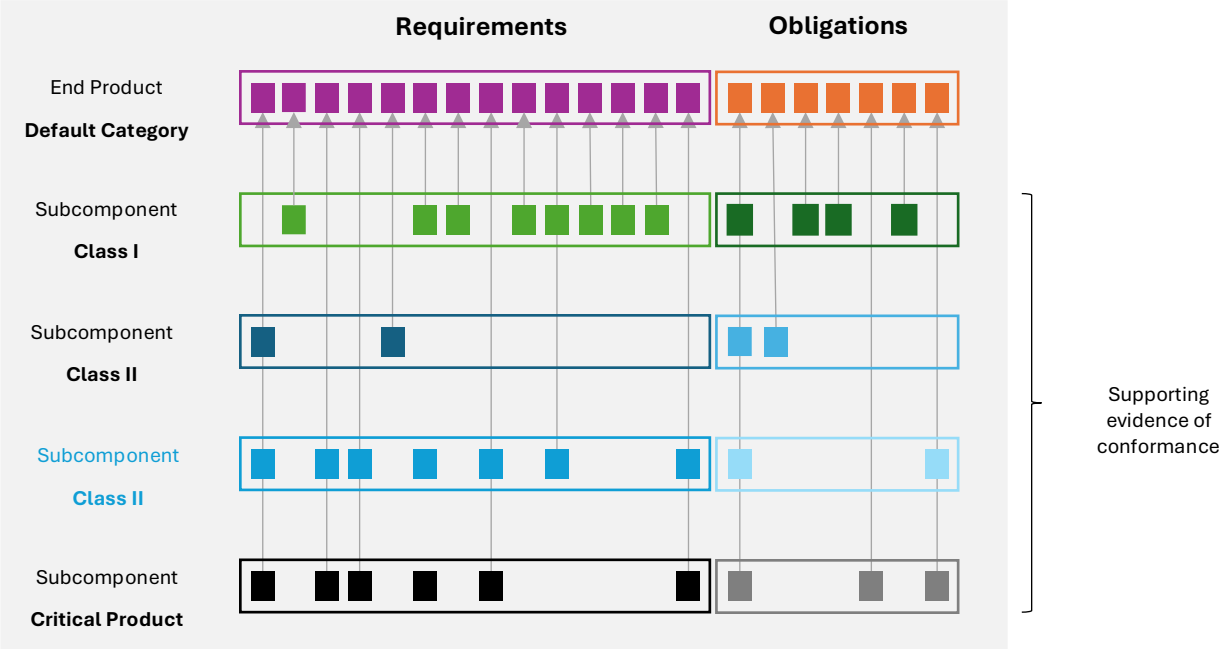

Figure 1. Example of CRA as a modularity exercise

For 3rd parties performing product assessment, the use of modularity has multiple benefits:

- Scalability. Every product is unique. Even across the same product types, each manufacturer is free to implement security on its way. It might be that the very same manufacturer has multiple implementations across product lines. All this reflects on the evaluators having to “learn” the product before they can test it. And yet, many of those products can have common components providing common functionality. A modularity approach hence is a scalable solution for assessing products.
- Efficiency. As per Figure 2, time is better used by evaluators focusing on the proper integration of secure (verified) components rather than looking to test every security functionality. When Product A has as many components as Product B but not much evidence beyond the “trust me” claim, the evaluator will spend additional time understanding how security works (learning the components). Product B has critical components recognized by the evaluator as “OK” (trusted) products. At least, the evaluator understands the security claims and their robustness and implementation of them. Creating assessment plans for the two scenarios is of a different magnitude. For product B, the lab focuses on proper integration rather than testing already certified capability. The subcomponent's security claims are standardized, reducing the effort for the lab and the developer and delivering higher assurance compared to a similar test for product A.

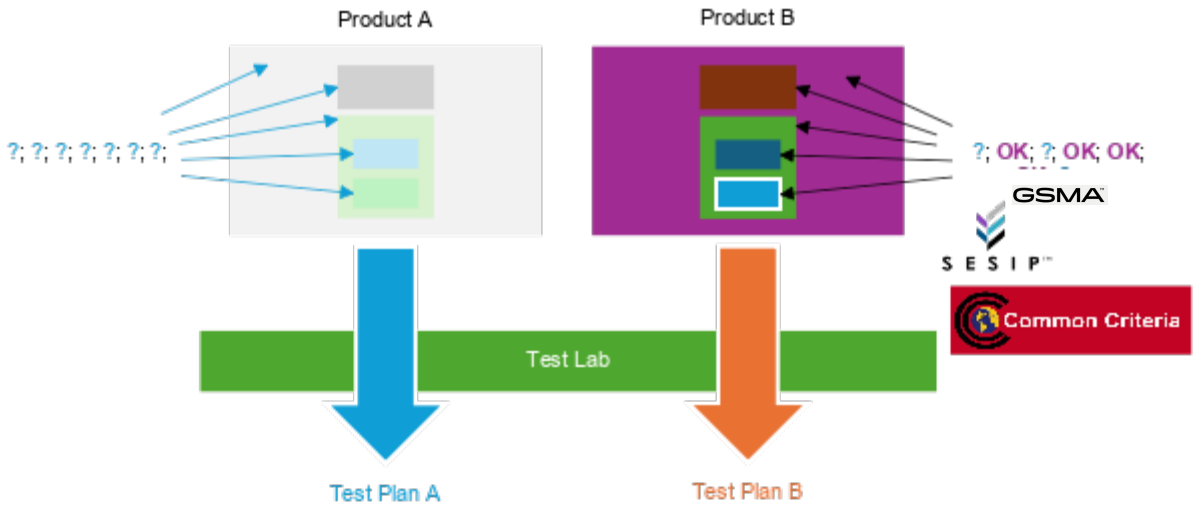

Figure 2. Test plans without (A), and with modularity (B)

There are other regimes outside Europe that manufacturers must conform with using 3rd party assessments, even if their product is in the CRA default category. While the CRA has the ambition to build MRAs, this can take time, and the use of modularity will help reduce the fragmentation of conformance claims that global manufacturers are facing. Besides national security policies, there are industry best practices for example the use of standards like IEC 62443-4-2 for the assessment of industrial equipment. The evidence presented in Product B from Figure 2, could be used in developing test plans that include CRA and IEC 62443-4-2 and a much more scalable and efficient way compared to the test plan from Product A.

Last but not least, equally important is to establish guidance for assessing the manufacturer's selection of components for specific use cases, connected to the security components' capabilities and the risk. Without such guidance will be difficult to establish when a manufacturer has fully complied with such obligation.

In summary, the use of modularity for addressing CRA conformance:

- Delivers additional assurance when the testing party does not test for robustness and implementation of the low-level security functions. Instead, verifies the proper integration of the components.
- Reduce time defining the test strategy, and tests to be executed.
- Standardizes security capability claims.
- Reduce interaction with the developer(s).
- Reduces OEM efforts (e.g. self-declarations).

Components security assurance mechanisms

In today's industry, there are well established and mature security assessment methodologies that can be reused for CRA conformance assessments for different component types. (EU)CC is commonly use mechanism for many high security applications and domains. As per Figure 1, a Secure Element in the Critical Product category from the CRA will serve as secure enclave of the device. Traditionally, and as acknowledged by the CRA text, those kind of components are evaluated with (EU)CC. However, under the CRA, with the large number of products and verticals under the scope, it's impossible to adopt one single approach. Flexibility and inclusion are required to address such variations and therefore it's important to have multiple evaluation methods as part of the CRA conformance toolbox.

EN 17927, the Security Evaluation Standard for IoT Platforms (SESIP) comes to complement CC for the substantial and basic levels of assurance for ranking validating component's security claims. EN 17927 can be understood by a broad range of audiences. Following the same security principles from CC in an optimized manner for the IoT market. Moreover, EN 17927 is designed for modularity. Both, for the security assessment of individual components and their combinations, for example Microcontroller + external secure flash + Operating System, and all the way to entire modules.

In addition to Common Criteria and EN 17927, PSA security certification program is widely and globally adopted. PSA provides range of security levels that can be applied to the broad range of connected devices corresponding to a range of security risk levels. The PSA Certified (TM) program (https://www.psacertified.org/) offers a wealth of resources for device manufacturers, silicon vendors, system software providers and IP providers. For example, the PSA Certified program uses EN 17927 as an assessment methodology for CRA relevant devices such as MCUs, MPUs, etc used in many products across many verticals.

Already today, GSMA eSA provides a Common Criteria based security certification scheme for eSIM (see https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/euicc-security-assurance-esa/). Beside serving as trust anchor for connectivity, additional security services can be offered by the eSIM for securing the services of devices.

With CC already in the CRA text, the adoption of the EN 17927, PSA Certified, GSMA eSA and other industry-driven mature security assessment initiatives supporting the development of standards applicable to Class II products, as well guidance documents (horizontal standards) specific to the use of modularity for CRA conformance claims, the industry will be ready for a

successful CRA implementation. Reflecting the nature of the various product types, and best practices in the industry applicable to each of them.

Call for action

Eurosmart members invite the European Commission to include the concept of Modularity in the upcoming Implementation Acts and formal Standardisation Requests for CRA standards.

There is a need to develop guidance, in the form of a horizontal standard addressing modularity. This standard will guide the use of security composition and reusability of security evidence from the essential requirements in products relying on the security capabilities of their components. Additionally, including modularity in the toolbox for Class II conformance mechanisms will complement the use of CC certified Critical Components, closing the gap required for efficient CRA conformance assessments.

While modularity is an efficient way to approach a successful CRA implementation, this paper does not intend to make the argument to claim it's the main or only method. Instead, the paper aims to highlight the relevance of the approach and the need to include it in the CRA.

Such guidance will support the development of specific vertical standards for products like Consumer and Industrial, with specific conformance claims for the CRA and other standards abroad, as well as the harmonized approach for 3rd party assessments as the selected conformance mechanism.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

EUROSMART
The Voice of the Digital Security Industry

Square de Meeûs 35 | 1000 Brussels | Belgium
www.eurosmart.com