EUROSMART
The Voice of the Digital Security Industry

Eurosmart welcomes the proposal for a Cyber Resilience Act

Eurosmart welcomes the European Commission's proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (the Cyber Resilience Act (CRA)).

Over the last decade, the European Union has been developing a solid cybersecurity legislative corpus which provides more legal certainty for the industry while increasing the digital security of ICT products and solutions for the benefice of European citizens. This new legislative proposal aims to complement and improve the enforcement of the existing and future EU digital security legal legislations (NIS directive, Cybersecurity Act and its related certification schemes, AI act, eIDAS, the EU Chips Acts and the forthcoming EU digital identity wallet)... Eurosmart, as the voice of the digital security industry, pays particular attention to all the initiatives which increase the security level of the Digital Single Market.

In this perspective, the definition and the adoption of rules for placing products with digital elements on the market to increase the cybersecurity level are paramount for Europe to be less dependent on non-EU technologies and the openness of the European digital market. In this respect, standardisation is a prime topic; the new European standardisation approach should be adequately developed to make the CRA successful. Until now, for most digital products, software and hardware, there was no guarantee for the consumer that the digital product they have in their hands meets a minimum set of cybersecurity requirements. In this respect, vulnerability handling requirements for providers of such products will contribute to increasing the level of security. Moreover, encryption as a way to ensure a high level of security is a core European concept, because privacy matters, this transversal requirement must be maintained in future policy discussions.

Software as a product

Eurosmart supports the European Commission's approach considering software as a product with the relative liability rules. It will bring more visibility to the whole cybersecurity value chain when placing on the market final goods relying or relying on software.

Consistency with eIDAS

The CRA provides a complementary approach to eIDAS, allowing wallet issuers to demonstrate compliance with both eIDAS and CRA requirements through a cybersecurity certification issued under the Cybersecurity Act. Eurosmart believes the European cybersecurity certification approach is an excellent option to support the presumption of conformity for such products. Moreover, these schemes will guarantee the right level of robustness for these critical products. Eurosmart encourages the Commission to identify, finalise or request a suitable cybersecurity scheme to support this approach[1].

Scalable cybersecurity approach

The scalable approach in the matter of cybersecurity goes in the right direction. However, the conformity approach is essentially functional and covers the robustness aspects of a product. Eurosmart welcomes the definition of two different classes of products; security requirements differ according to their criticality and environment; the digital security industry will carefully assess the applicable requirements and the type of products falling under the different classes. As already stated in previous Eurosmart's feedback[2], the European Cybersecurity Certification Framework is an interesting tool to complement this approach and support the development of future schemes to ensure the presumption of conformity with the CRA requirements.

CRA's provisions to be clarified

Cybersecurity certification for critical products

When referring to cybersecurity certification schemes for Critical products with digital elements, the Commission should systematically consider the Cybersecurity act (CSA) level "high" to provide a presumption of conformity with CRA requirements. The CSA level "high" involves mandatory penetration testing, which is the only way to seriously evaluate the robustness of critical products with digital elements. Moreover, identifying any potential cybersecurity certification candidate schemes should involve the different stakeholders of the Cybersecurity certification Group.

Cybersecurity certification for digital products

The European certification schemes at "Substantial" and "basic" levels provide the level of assurance required for demonstrating conformance once the baseline requirements are established, with potentially new certification schemes for different product types as described by the CRA. Moreover, it provides the mechanism for the reusability of evidence across the European cybersecurity corpus. Additionally, Eurosmart encourages different standardisation initiatives to support these certification schemes.

---

[1] The EUCC scheme is a good candidate to cover some part of the EUIDwallet, Eurosmart encourages the Commission to adopt the candidate scheme to support this set of legislations. Additional scheme to support other parts of the EUIDwallet should be explored.

[2] See Eurosmart's feedback on New cybersecurity rules for digital products and ancillary services (May 2022)

https://www.eurosmart.com/cyber-resilience-act-cra-new-cybersecurity-rules-for-digital-products-and-ancillary-services/

CRA and Radio Equipment Directive

The CRA will consider a "radio-equipped product" as defined by the Radio Equipment Directive (RED). A standardisation request addressing the cybersecurity aspects has been sent to CEN/CENELEC, and standards are under development. The Commission should clarify the statutes of the RED requirements, which will be applicable as of the 1st of August 2024[3].

Standardisation approach

The European Commission could rely on the definition of "Common Specifications" when the edition of harmonised standards is too complex to put in place. In such circumstances, the edition of "Common Specification" must involve the National Standardisation Bodies of the Member States and the European Standardisation Organisations (ESOs) representatives following a stakeholder's consulting period.

Labelling and Information to end-users

Additional paths should be explored to raise end-users' awareness regarding the security level of products with digital elements. For instance, Cybersecurity certification schemes may provide labelling. This type of label may be implemented through the CRA to provide information about core security functionalities and the class of the products.

Implementation period

The implementation period of 24 months after entry into force would be a challenge for the European industy.

[3] Commission Delegated Regulation (EU) 2022/30 with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f) of the Radio Equipment Directive