EUROSMART
The Voice of the Digital Security Industry

Evaluation of Regulation (EU) No 1025/2012

Addressing Security Standardisation Challenges in the EU

Eurosmart, the leading association representing the digital security industry in Europe, welcomes the initiative based on the update of the European Standardisation Strategy to evaluate the Regulation (EU) No 1025/2012, especially in the light of supporting compliance of digital products with newly created essential requirements.

The development of harmonised European Norms (hEN) requires a clear distinction between security and safety. Although both domains aim to mitigate risk, they address fundamentally different aspects: safety deals with hazards, while security addresses threats. The confusion between these two concepts in regulatory frameworks can hinder the effectiveness and evolution of hENs, especially in the context of rapidly advancing technological landscapes. This paper argues for the necessity of recognising the distinct nature of security in hEN development, leveraging existing industry-driven standards to create efficient and effective norms to support the correct implementation of the cybersecurity regulatory frameworks.

1. Safety is not (Cyber)Security

Safety is traditionally focused on preventing accidents and minimizing hazards that may occur inadvertently. This is the base of the ‘New Approach’[1] and the ‘New Legislative Framework’(NLF)[2] dealing with safety of product and market access. In contrast, security is concerned with protecting systems from intentional threats posed by malicious actors. This fundamental difference, the intent behind, highlights that risk in the context of security implies an intentional element that safety does not encompass.

Today’s EU market access rules encompass cybersecurity rules with a safety-based approach. The translation of “essential requirements” into hEN providing legal certainty is still predominantly built around safety, stemming from legacy frameworks covering safety

[1] The 'New Approach' laid down in Council Resolution of 7 May 1985 limits the content of legislation to 'essential requirements,' delegating technical details to European harmonised standards. To this end, the formulation of European standardisation policy is necessary to support the legislation.

[2] The ‘New Legislative Framework’ adopted in July 2008, is built on the New Approach and consists of (1) Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products, (2) Decision 768/2008 on a common framework for the marketing of products and (3) Regulation (EU) 2019/1020 on market surveillance and compliance of products. A set of 26 sectorial legislations and the Cyber Resilience Act rely on this framework.

requirements. However, as foreseen by new cybersecurity regulations based on the NLF must evolve to adequately address the unique challenges posed by security threats. Treating security as an extension of safety can create a misleading sense of security in the market, undermining the integrity of products and systems.

Given that cybersecurity is a relatively new domain within Union harmonisation legislation and in hENs, establishing objectively verifiable requirements and assessment criteria for hENs stand out as a paramount challenge for the European Standardisation Organisations (ESOs). This challenge became evident during the development of Radio Equipment Directive (RED) hENs and remains a critical element for the European Commission, which aims at preventing manufacturers from making "key technical decisions" during the implementation of harmonised standards.

The relevance of the security posture of an ICT product, as well as cybersecurity in general, lacks physical measurability. Unlike traditional physical metrics, there is no direct equivalent tool in digital security domain for ensuring quantifiable measures in an objective manner. This inherent challenge has been underscored by the National Institute of Standards and Technology (NIST), which has launched a program to support cybersecurity measurements[3]. In cybersecurity, evaluating test results hinges upon the technical implementation and the knowledge and know-how of the evaluator regarding what constitutes adequacy and appropriateness for a specific product within a particular environment.

2. Challenges in Security Standardisation

2.1. Guidance for security standards developments

The development of hENs addressing security aspects requires a more specific approach while still providing a generic assessment framework to develop technology-neutral standards. Based on the experience from the RED hENs development, these security standards cannot be developed in the same way as traditional safety standards; they require more time and resources. In this respect, as requested by CEN-CENELEC Working Group 8 (WG8), legal guidance from the European Commission is necessary to determine the exact level of acceptance. Specifically, what constitutes an adequate and appropriate level of objectivity? And how can this level of objectivity be measured?

2.2. Streamline security standards development and provide more resources

Developing security standards is a resource-intensive process, complicated by a shortage of professionals and the extensive collaboration required among various stakeholders. Both public and private sectors need to converge on standards that can effectively claim conformance with existing policies, which is often a complex and costly undertaking.

Multiple technical groups and organisations are involved in developing security standards, leading to fragmentation and lack of communication. The European Standardization Organizations (ESOs) must align their work with policymakers' expectations, balancing objective standards with the inherently subjective nature of security threats.

[3] NIST Performance Measurement Guide for Information Security – November 14, 2022 - https://www.nist.gov/cybersecurity-measurement

The decision-making processes for hENs, ENs, and other technical deliverables differ among ESOs4. However, the same decision-making process should be applied consistently for key milestones. Additionally, in various approval procedures, non-EU National Standardization Bodies are asked to cast votes that influence the adoption process of the standards.

The European Commission should enact new provisions to ensure that important decisions related to hENs and related deliverables are voted on exclusively by representatives of the EU's National Standardization Bodies. This approach must be clearly reflected in the ESOs' Rules of Procedure.

3. Leveraging Industry-Driven Standards

Several industry sectors have successfully developed adopted and implemented security standards through industry-driven associations. Some examples of them are:

- **Mobile Communications:** The GSMA has developed comprehensive security standards for mobile networks.
- **Payment Industry:** EMVCo has established robust security standards for payment systems.
- **Semiconductors:** The SESIP standard (EN 17927) provides a security framework for semiconductor products.
- **Wireless Charging:** The Qi standard ensures secure wireless charging solutions.
- **Automotive:** The Car Connectivity Consortium has developed digital key standards for automotive security.
- **Consumer Devices:** The Consumer Standards Alliance Product Security Working Group has created security standards for consumer devices.

Relying on these existing industry-driven standards as a baseline for hEN development can significantly reduce time and costs. These standards, already proven effective in their respective sectors, provide a robust foundation upon which new standards can be built, ensuring compliance with the Cyber Resilience Act (CRA), the Radio Equipment Directive (RED), and other relevant regulations like the AI-Act, NIS2, and eIDAS.

[4] Eurosmart's Feedback on the revision of the Standardisation Regulation & Standardisation Strategy, 22nd September 2022, https://www.eurosmart.com/feedback-on-the-revision-of-standardisation-regulation-1025-2012-the-standardisation-strategy/

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