EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Certification

Challenges ahead for the roll-out of the Cybersecurity Act

WG1 – Standardisation, certification and supply chain management

December 2020

www.ecs-org.eu

About ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg1_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information is limited to ECSO WG1 members

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

Copyright Notice

Table of Contents

1. Introduction

This document originates from the answers ECSO members gave in response to an internal survey meant to shed light on several topics in support the Cybersecurity Act, the forthcoming European certification schemes, their priorities and their implementation.

The objective is to understand the main challenges that could hinder the usage of future European cybersecurity certification schemes across industries. Thus, the goal is to identify the necessary future steps and aspects that ECSO WG1 should investigate in the coming months in addition to foresee the potential impact on the market.

This document does not discuss the potential consistency among the Cybersecurity Act, Directives and Regulations.

2. Certification Framework consistency

Ensuring the consistency of the European cybersecurity certification framework is key to setting trustable and reliable certification schemes that are recognised and used by all stakeholders. The overall objective is to define a cost-effective certification process for any applicant. Such an objective is not easy to tackle due to the different Security Assurance Levels, the diversity of applications, including products, systems and services potentially subject to certification, as well as the numerous technologies, the diversity of market sectors and their stakeholders.

If we consider maximum re-use of solutions and technology (services, products, etc.), a horizontal view, i.e., sector agnostic, should be the preferred option to help saving costs, but also simplifying choices when deploying secure ecosystems. This should be **balanced against the considerations of sector-based specificities** where unique aspects of different sectors may need to be addressed. The sector and the intended use are relevant to determine what needs to be certified and how it should be certified, thus they should be reflected in the cybersecurity evaluation.

Ensuring similar or comparable levels of assurance across schemes is challenging as the resulting installation of the same product in a different operational context may be in widely different risk environments that do not correspond to the operational context of the risk evaluation used to identify the assurance level, reducing the value of a risk-based approach.

The focus should be on **providing guidance for the consistent mapping between the risk and the assurance levels**. Further, although such a matching is needed, it will create its own challenges and complexity unless there is a consistent method and approach to risk evaluation. Otherwise, different risk methods may result in different interpretations of the resulting risk level and, as such, create a discrepancy in any mapping to assurance level.

Framework consistency shall be based upon pillars and/or best practises in developing (scope and technical requirements) and implementing certification schemes (certification methods and processes) including a governance aspect between all stakeholders.

These pillars shall be addressed through:

- A more precise and consistent definition of the Security Level of Assurance (more detailed than the CSA and especially for Substantial and Basic) to ensure its consistency throughout the different sectors and to be understandable by the end users, the manufacturer, the public and the consumers (not reserved to cybersecurity experts).
- The promotion and enhancement of international and/or recognised standards even if adapted to cope with Basic and Substantial security level of assurance to avoid duplicating or multiplying technical assurance requirements and to ease their implementation and so guarantee consistency across security assurance levels.
- A risk-based approach to map Security Assurance Levels with the Cybersecurity Act levels Basic, Substantial and High.
- Harmonisation of risk analysis methods
- Common or similar methods and methodologies of assessment and testing (including criteria or topics to be checked, evaluated or tested) to demonstrate the compliance against the technical requirements for a defined assurance level. For instance, in term of depth and rigor, i.e. the degree of effort and depth of the assessment for a Substantial level in a given scheme A should be "equivalent", in the same order in accordance to best practices of the domain, to those for the same level in scheme B. This aspect shall also include the evidences, the acceptable means of compliance.
- Harmonised approaches and processes of certification bodies and testing labs (Conformity Assessment Bodies) through a governance (accreditation may be a way) and a market surveillance to ensure consistency of certification and dissemination of expertise and state of the art in cybersecurity certification.

3. Composition

The European cybersecurity certification framework will include several certification schemes for ICT products, services and processes: horizontal such as the EU Common Criteria (EUCC) scheme or covering specific verticals such as Cloud services, IoT or 5G. But these verticals could be used as horizontal schemes that are then specialised for specific market sector such as medical devices, smart meters or connected and automated mobility. Therefore, the ability to certify a product "by composition" will play a key role for the cost effectiveness and usability of the EU certification: e.g. an IoT system may rely on a certified IoT device and a certified cloud service, the IoT device may rely on certified hardware component, etc. ECSO has published a document on product composition[1] that could support that objective and set important directions to be considered for future work.

Security is known to be non-compositional in general, i.e., combining "certified 'secure' products" does not result in a "secure system" or "secure connected product". They are composed of many

[1] European Cyber Security Organisation (ECSO) WG1, "European Cyber Security Certification: Product Certification Composition," November 2020

parts and components, developed by different actors, and reused in multiple products or systems. More and more products are based on ‘platforms’ providing security foundations not developed by the product manufacturer itself. So, a flexible methodology for efficient evaluation and certification based on reuse of evaluated and certified foundations is a must. Nevertheless, there are several aspects that need to be considered: a system composed by devices could be composed by several components with different levels of security, so security composition could be a desirable design feature, as well as multilayer assessment, dealing with the different threats and risk levels that could be derived from each layer and from the context in which the system operates.

ENISA has been tasked with two certification schemes, SOGIS Common Criteria (EUCC) and Cloud Services. No matter how secure an individual component certified under the EU Common Criteria based certification is, any system as complex as a Cloud Service cannot be solely certified by plugging individual certified components together. However, using individual certified secure components may help in reducing the workload when evaluating the security of a Cloud Service. Once an evaluation of a service reaches the granularity of an individual component (including the cloud server and the corresponding physical site) already certified to an evaluation methodology such as EU Common Criteria, then the service evaluation can at least in part reuse the results of the components certification claims.

Cloud services is a new and challenging certification domain that could explicitly use/refer to composition, introducing a requirement for using a EUCC certified devices in certain areas, such as identity or payment. For example, certifying a cloud service might require evaluating that the cloud service provider secures the authorisation and authentication of who is accessing the data or taking actions and a certified EUCC device is a proven solution to attest the identity/authentication/integrity of objects/persons.

The system should be considered as "whole" with a risk analysis, that takes into account the use cases (that will depend on the cloud service model, SAAS, PAAS, IAAS). The security objectives and corresponding security requirements will be derived for each use case based on the threat model and corresponding risk analysis. Each side (the device and the cloud platform providing the service) will have to fulfil a set of security objectives/requirements (implementing the security functionalities) and complying with the assumptions of the other side, e.g. assumptions about the communication protocol security level. This is independent from the specific scheme used to certify each side but requires guidelines about the achieved assurance level of the whole system (composed target).

The certification composition activities will cover several phases of the product life cycle such as risk analysis, the secure design, manufacturing and delivery but also the operational environment, and maintenance until the end-of-life.

The Role of the system integrator

According to the principle that the security of the final solution that the integrator is building depends on the weakest component, then the individual certification of each components, according to a specific scheme and at a specific assurance level, will generally provide a given assurance level equivalent to the lowest assurance level. If we assume that each product/components certification provide assumptions/security objectives about the environment (in which it will be integrated), the system integrator will have to check the compliancy and that the integration does not increase the attack surface, i.e., it will not introduce additional vulnerabilities.

The integrator has to perform the threats and risk analysis of the global solution to ensure that the products/components s/he integrates fulfil/contribute to the risk mitigation. Ideally, the choice of the components derives from a secure design and a security architecture for which components/devices are best suited for addressing the security needs of that particular solution. The procurement department and the CISO could play an important role in defining the responsibility of the system integrator.

Leveraging standardised process for composition

Considering the challenge to achieve end-to-end security, the end-to-end certification targeted by the composition, and, the activities to be performed for certification by composition, the availability of a standardised process for composition may accelerate the acceptance of the certification schemes that are to be defined. Like the horizontal EUCC scheme, specific methodology and process for certification of a system/product using certified components facilitates the interactions between the suppliers and the final product integrator. Building and certifying a secure solution made of secure products, secure cloud, and secure infrastructure requires a process for composition to drive at least the process of deriving a level of assurance from assurances on each components of the solution architecture.

Obviously, specific domains like cloud services will benefit from a process for certification composition as at the contrary of other well-known ICT technical domains, the target of the certification/certification scope, the service, will depend on the architecture model (IaaS, PaaS, SaaS, etc) and on several kinds of “product”/”system”. Defining a composition process in that domain as there is a benefit in clearly defining rules and processes when developing cloud service, ensures that every important aspect gets assessed and implemented in a manner that complies with best practices.

4. Priorities for certification schemes

ECSO members highlighted several needs and considering the importance of a prioritization for the work on new candidate schemes, ECSO suggests that economical & societal value is given key consideration both with respect to the general public and in favour of the fragmentation reduction in the Digital Single Market.

ECSO understands that focus should be given on the reduction of societal and sectorial risk, with emphasis on critical services, society security, health and personal data. Those segments can immediately benefit from secure products and the implementation of secure processes and services.

It is understood that a continuous risk-based process for the implementation of an information security management system (ISMS) and associated certification in corporations can produce a significant positive impact on the Digital Single Market, decreasing exposure to threats and contributing to overall supply chain security.

Looking at the market proposed value ECSO suggests that **two main actions should be taken:**

- First axis is at **the base of the Digital Single Market**, improving the overall consumer product **security at basic/substantial levels** and putting in place **the needed ecosystem**

to encourage, define, monitor, assess and help companies improve the security of their products.
The usage of automated tools, e.g. testing, can speed up the whole process and contribute to the certification simplification.

- The second axis should focus on the family of security or non-security products since the EU has the strategic intention to be the **global reference in terms of reliability and resilience**.

Some areas highlighted by ECSO members are:

- SDL/Secure Development Lifecycle process
- 5G Component, product (SW, HW), systems and services
- Industrial and consumer IoT devices
- Healthcare devices, services, organisations (e.g. hospitals)
- Industrial environments
- Smart Buildings
- Critical infrastructure and ICS/SCADA devices.

The number of future Cybersecurity certification schemes should match the European market needs, with a strong effort for simplification & mutualisation. A dedicated gap analysis from proposals and existing EU schemes must be observed, not only for technical reasons but also for economic reasons.

Horizonal and vertical schemes

Efficiency and cost effectiveness should be key forces in the EU certification framework, **a reduced amount of horizontal and vertical schemes** should be preferred in order to have a cost-efficient approach for all parties, such as scheme operators, applicants, etc.

The technical reasoning for creating additional specialized schemes should be systematically aligned with the capacity to address the same problems in a horizontal scheme using a detailed security problem definition.

Schemes must allow composition and reuse of evidence in order to have flexibility (to adapt to application requirements) and transparency to ensure consistency in assurance. This is feasible with a scheme methodology designed/suited/adapted for composition. Vertical schemes must define the security needs/objectives in a risk-based approach (involving the risk-owner/industrial) allowing the vendor to instantiate the right security functionalities certified in a horizontal way and complete the threat model coverage in a vertical scheme by adding specific requirements.

Vertical certification schemes are **fundamental to address the specific technical, operational and regulatory requirements** of the targeted market. Caution should be observed when there are already mature market practices, in which case these should be prioritised.

For vertical certification schemes, the security requirements and the corresponding evaluation methodology should be defined with the specificity of the corresponding vertical/industry that has an impact on the feasibility of the implementation of those requirements by the products or systems. The threat model and the risk exposure may depend on the vertical, e.g. automotive threat model for ICT in-Vehicle components or an Industrial systems (SCADA) where security requirements and evaluation methods are specific to this industry. The scheme per vertical should rely/use the existing industrial (security) standards if any as that is the only way to avoid fragmentation and to ensure **acceptance by the corresponding market.**

5. Conclusion

The challenges herein discussed do not address policies other than those covered by the Cybersecurity Act, but they consider the implications of the roll-out of the European certification schemes to the market for addressing security. Moreover, this document has not discussed the potential consistency among the Cybersecurity Act, Directives and Regulations addressing sectorial IoT devices, services and systems, which forms part of future activities. Consistency is important and should be maintained to avoid harmful overlaps or contradictory approaches for addressing cybersecurity. For example, the introduction of cybersecurity objectives in regulations that need to be enforced with legal certainty may prevent risk-based approach and create difficulties in security assessment.

This document has indicated some important pillars to help understanding the interaction among the different certification schemes and sector needs. This is key to paving the way to a better understanding of the market adoption of the different schemes. In terms of market impact and potential adoption of certification schemes, one of the challenges that has been identified is the definition of vertical and horizontal certification schemes according to the different market segments, also considering the different regulations dealing with safety and regulating specific sectors. This aspect will be addressed in future documents.

ECS

EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU