European Semiconductor Industry Association

POSITION PAPER

on the Union Rolling Work Programme for European Cybersecurity Certification

Brussels, 15 July 2020

Introduction

The European semiconductor industry is market leader in offering cyber-secure, innovative hardware solutions that enable cutting-edge technologies of the present and future. They provide the basis for innovations in a wide range of industries such as automotive, industrial, consumer electronics & mobile communications, health and energy. With digitisation and connectivity pushing deeper into the fabric of European society, the expectations of and demand in cyber-secure semiconductors shall continue to grow.

In a digitised world with ubiquitous connectivity, security and privacy are becoming a key concern for businesses and citizens alike. With more & more connected devices, the need for properly certified "*security by design*" becomes essential in order to create trust in smart connected solutions. European encryption methods are globally recognised worldwide already for their high security standard. Pan-European certification schemes are going to promote the unique selling point of cybersecurity solutions "*made in the EU*" even further.

Nonetheless, when assessing the need for new schemes, the Union Rolling Work Programme (URWP) for European Cybersecurity Certification should refrain from solely adding certification schemes for various technologies. Otherwise, the framework may produce a very fragmented and burdensome certification landscape that would thwarts the objective of increasing security for information & communications technology (ICT). Instead, the interconnection of technologies ought to be central to ensure that underlying generic component certification can be re-used across multiple use cases. The URWP should focus on composition, integration and merging of existing certification schemes.

I. 5G networks

Semiconductor companies in Europe are market leading in the power and radio frequency (RF) segments. When it comes to 5G, all products related to the Internet of Things (IoT), industrial applications, traffic, health care, and generally supported by connectivity will benefit European citizens in their daily lives to improve everything from business to private affairs.

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

However, 5G connectivity is a complex subject matter and any suggested certification scheme must look at system as a whole and break it down into key critical security points. Existing certification schemes must be tested and assessed whether they interlock and work together to provide verification that 5G security claims are true, robust and verified.

It is most essential that European certification is consistent and aligned with assurance schemes of the 3rd Generation Partnership Project (3GPP) and the Global System for Mobile Communications Association (GSMA) to prevent duplicating evaluation & certification efforts. The Network Equipment Security Assurance Scheme (NESAS) alone, however, is heavily weighted to process, not covering how the 5G network components are security tested & fit together. ESIA supports the use of Common Criteria (CC) for critical elements providing hardware security foundations[1]. For full 5G products or systems, lightweight evaluation and certification methodologies (enabling easy composition with CC certified security foundations) should be considered to reduce time to market.

II. Industrial & automation control systems

Industrial & automation control systems (IACS) and industrial operational technology are crucial areas that must be protected to ensure cyber-resilient EU industries. A widely used standard is IEC 62443, which has initiated an EU pilot scheme proposal with scalable assurance. It does, however, rely heavily on process & good practices. In addition, IEC 62443 lacks robust & clear security test policy and strategy. Hence, the URWP should examine how other public certification standards can be re-used to align the test proof required.

ESIA welcomes the establishment of a minimum common level of security through a risk-based certification process. It should be stressed that composition plays a central role in industrial product certification (this is aspect is also missing from IEC 62443). It is critical to minimise the efforts for product developers, allowing the re-use of already certified parts of the product (e.g. a certified platform, a secure element, etc.).

III. Lightweight evaluation schemes

ESIA encourages the composition and re-use of methodologies and standards that are already in use by the industry to maximise consistency & coherence. No new schemes should be generated; instead, lightweight schemes should concentrate on the concept of baseline security protection profiles that can be used in existing schemes. Efforts would be better invested on protection profiles and test approaches rather than generating new schemes.

[1] For instance embedded Universal Integrated Circuit Cards (eUICC) or embedded Secure Elements (eSE).

IV. Secure development lifecycle

ESIA supports the URWP intention to provide standards and certification for process of development (i.e. lifecycle, "*security-by-design*") with a risk-based approach. This should be developed consistently with standardisation of products' security capabilities. Moreover, certification should allow the direct re-use of already granted certifications, such as Senior Officials Group Information Systems Security (SOG-IS) Minimum Site Security Requirements (MSSR) or GSMA Security Accreditation Scheme (SAS).

Nonetheless, secure development process standards are not sufficient to give full security proof and verification, as certification relies heavily on the trust of a developer. Proof that a given product followed the process and that its security claims are justifiable should also be required.

V. Commercial IoT products

ESIA cautions that commercial IoT products present a 'blind spot' as regards certification. A trusted label or methodology is needed to harmonise security expectations. At present, IoT schemes tend to be narrow in scope, light on test, not user-friendly, or rely on self-certification. ESIA encourages a lightweight approach that is harmonised around a set methodology such as Security Evaluation Standard for IoT Platforms (SESIP), developed by industry as well as Conformity Assessment Bodies (CABs) and National Cybersecurity Certification Authorities (NCCAs). A common standard should be agreed upon and elaborated further into a trust label in Europe.

VI. Further discussion

Currently, ESIA deems it too early to consider certification for an immature, developing technology as artificial intelligence (AI). At the same time, however, it is important that AI is considered as an important piece within the larger cybersecurity landscape. User data must be guarded, while supervision is crucial as to how AI models are built, protected and used. This is not only a security issue, but also a concern in terms of ethics and liability. The Stakeholder Cybersecurity Certification Group (SCCG) should work alongside the European Union Agency for Cybersecurity (ENISA) and the competent Directorates-General in the European Commission to examine all aspects of AI and put forward key recommendations for any European project that utilises the technology.

ESIA considers cryptography to be a security function that should be addressed in a generic scheme, as included in foundational security features. Harmonised and agreed cryptographic primitives should gather a common understanding of strength of function, implementation and key lengths (including agreed random number generation methods). Moreover, to ensure harmonised & correct implementation of cryptography across the EU, ESIA would suggest the implementation of a similar validation programme to the Cryptographic Algorithm Validation Program(CAVP) of the U.S. National Institute of Standards and Technology (NIST). This would also neutralise the reliance on NIST as the go-to for cryptographic commonality.

For further information:

Hendrik Abma
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 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.