# POSITION PAPER ON THE CYBERSECURITY ACT

Eurosmart, the association representing the European digital security industry, welcomes the adoption of a new European Cybersecurity Act, which includes a new harmonised security certification and labelling framework.

Eurosmart fully supports the Commission's proposal for a cybersecurity act granting ENISA a key role as a cybersecurity agency with full operational capabilities. The creation of a European Cybersecurity Certification Group in the European cybersecurity framework is also welcomed by Eurosmart as it will foster enhanced coordination of existing security certification schemes.

The European worldwide leadership of digital security industries and associated eco-systems is dependent upon the very high security level ensured by the current SOGIS MRA ("Senior Officials Group Information Systems Security- Mutual Recognition Arrangement") certification scheme.

This Digital security technology is a unique European success, more than 120 countries in the world use it for securing their electronic passport, all well-known high-end smart phone manufacturers use it to protect their critical assets, as does the European Parliament with the latter using them for electronic voting systems.

It should be noted that even the US Department of Defense (DOD) is using European technologies (secure elements) to protect their critical infrastructure and that NATO uses European technologies certified by SOG IS MRA in Europe and FIPS in the USA. Products that are currently in use have both certifications.

It is of the utmost importance that high performance levels are maintained in order to counter potential attacks on the new European cybersecurity certification scheme and to preserve European leadership via an EU security eco-system which consists of:

- Providers of secure hardware-based products;
- Encryption providers (local & cloud based);
- European High Security Hardware (HSM) providers;
- European Mobile operators, to securely manage network authentication;
- Research labs
- The cryptographic community – a large part of the European cryptographic community is working for European smart industry and its eco-system;
- Existing pen testing groups;
- Europe's existing accredited labs (with some pen-testing capabilities).

The European Union should build on Europe's unique worldwide expertise to maintain a high level of encryption resistance and high security levels for electronic identification, electronic authentication, web and cloud electronic services and electronic signatures.

SOG-IS mutual recognition is operational in the EEA and is processing various security products in a range of IoT domains, such as:

- Homeland security with secure *travel documents* and secure *border control;*
- Security on the highway with electronic *tachographs* for lorries and buses and *digital driving licenses* for citizens;
- Digital identity documents in the public sector for web and cloud applications with *national eID-Cards* and *residence permit cards* for 3rd country nationals.
- Finance with *debit* and *credit cards;*
- Health with health and professional cards & HSMs;
- Transport with electronic vehicle registration cards;
- **Secure communication** with embedded ***TPM*** **or secure elements in** PCs/laptops/tablets, which are required for MS WINDOWS 10 and higher.

***Eurosmart also wishes to express the following concerns about the current Cyber Act:***

1) Eurosmart highlights the need for vigilance in order to ensure a smooth transition from the existing SOGIS MRA scheme towards the future European schemes that should have the SOGIS MRA principles in a dedicated appendix of the Cyber Act regulation from day one. We should also recognize the strategical role of the existing national security agencies in the past 20 years in creating the best in class temper resistance cryptographic devices and software and services.

   Eurosmart advocates for an evolution of mutual recognition arrangement to all Member States, without jeopardizing the quality of the evaluation's requirements and methodology.

2) Certification versus Labelling:

   In the proposed regulation, only cybersecurity certification is described with no mention of the notion of labelling.

   As regards consumers and citizens, and as an additional approach, the creation of a European Union trust label can raise awareness of cybersecurity aspects pertaining to trust, privacy and confidence. Raising consumer awareness of security aspects will enhance confidence and trigger a market demand for connected devices.

***Eurosmart also has some questions for the co-legislator:***

1. In the European Accreditation Agreement (referred to in Regulation (EC) 765/2008) **more than 36 countries are full members**. How can we limit this to the 28 EU Member States (soon to be 27)?
   a. Does Conformity Assessment Bodies in non-European Countries that are full members of the European Accreditation perform a European Certification on a given product?
   b. Consequently, what would be the definition of a European CAB?
   c. And what about the definition of a European Country?

d. Would non-EU countries covered by the EA agreement have to create their own National Certification Supervisory Authority (NCSA)?

e. Would such a National Certification Supervisory Authority have some "power of investigation" vis-a-vis a foreign CAB? And the EU CAB?

f. How could non-European Standards (e.g. FIPS/USA, GHOST/Russia, SCOSTA/India, OSCCAR/China) be integrated?

g. How could ENISA ensure the appropriateness of and conformity with international standards used in (already) approved schemes?

2. The PWC study SMART no 2016 - 0029 that was used to perform the Impact analysis referred to several "errors" **in the SOG-IS-MRA whilst** the latest study on ENISA (published on the 19th of September 2017) is much more complete:

   a. Why was the ENISA study not published earlier so that it could be used in the impact assessment?

   b. What form will the submission of a list of errors to the Commission, Parliament and Council take? Eurosmart will be preparing and publishing some documents to highlight these "errors" in the coming weeks.

3. How can a fair & transparent process be ensured during the preparation of the security certification schemes?

In the proposed governance scheme there is no counter-power to ENISA and the selected sub-contractors would be mainly consultants (as defined in the PWC Impact assessment).

How can we mitigate the risk of experienced lobbyists seeking to influence the preparation of the security certification schemes whilst showing disregard for the interests of the European SMEs that are at the core of the current EU cyber security expertise in EU Member States**?**

4. How can we define a "European Association"?
5. How can we ensure that ENISA is transparent?

To ensure transparency in ENISA's determination of the stakeholders who will review the proposed certification schemes, we should invite the Council & the Commission to certify European stakeholder associations to ensure that they actually represent European industry and thus mitigate the risk of a consultancy firm misrepresenting European interests.

## *About Eurosmart*

*Eurosmart, the Voice of the Digital Security Industry, is an international 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.*

*Members are manufacturers of smart cards, secure element, semiconductors, secure software, security evaluation laboratories, High Security Hardware, Biometric technology providers, terminals, system integrators, application developers and issuers who work in dedicated working groups (security, electronic identity, communication, Cybersecurity, marketing). Members are largely involved in research and development projects at European and international levels.*

*Eurosmart members are companies (**Fingerprint Cards**, **Gemalto**, **Giesecke & Devrient**, **GS TAG**, **Idema**, **Imprimerie Nationale**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), laboratories (**CEA-LETI**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).*


***Press contact:***

**Pierre-Jean VERRANDO**

Director of operation

Mobile: +32 471 34 59 64

**EUROSMART**

Rue du Luxembourg 19-21 | B-1000 Brussels | Belgium

eurosmart@eurosmart.com

Tel: + 32 2 506 88 38 - Fax: + 32 2 506 88 25