



## Security certification and labelling

*Eurosmart's response to the Inception Impact Assessment of the European Commission on a proposal for a Regulation revising the ENISA regulation (No 526/2013) and laying down a European ICT security certification and labelling framework*

---

### Foreword

Eurosmart welcomes the European Commission's initiative as presented in its inception impact assessment and shares its view on the need to address the current fragmentation at both governance and market levels. Our association is fully involved in the current EU debate on ICT security certification and has been championing a meta-scheme approach in several EU working groups such as ECSO. Moreover, in addition to a European ICT security certification framework, Eurosmart supports the adoption of a mandatory EU labelling scheme "*Certified in Europe*" built on established security requirements and recognised certification schemes. A European ICT security certification and labelling framework will boost confidence, enhance visibility amongst users as well as equipment manufacturers and thus reinforce trust in the market.

### 1. On the role of ENISA

Eurosmart is strongly in favour of establishing ENISA as a veritable "central agency", as outlined in options 2 and 3. There are many initiatives addressing ICT security standardisation at the European level (the European Commission, the MSP for ICT standardisation, ECSO, AIOTI, etc.). As the European Commission rightly states, this multitude of initiatives constitutes one "dimension" of the current fragmentation. ENISA should play a more active role in coordinating such initiatives and therefore its remit should be more specific and its resources enhanced.

However, as stated in the NIS directive, the security of network and information systems is primarily the purview of national authorities. Due to the scale and the cross-border nature of cyber threats, new missions and enhanced capabilities should be given to ENISA to enable it

to perform the tasks outlined in options 2 and 3. Eurosmart supports the idea of moving from “cooperation” towards a more integrated model but believes that ENISA’s full capabilities to detect and respond to cyber threats should be established without prejudice to the role of the Computer Security Incident Response Teams (CSIRTs). The new governance model that the European Commission intends to propose should avoid any overlap as this could fragment the decision making process still further.

## **2. On certification and labelling**

The increasing number of domestic schemes leads to the distortion of the digital single market. Furthermore, some of these schemes are not compliant with international standards, thus preventing companies from accessing foreign markets as they have to comply with different methodological and evaluation criteria.

Eurosmart supports the creation of a European institutional framework for ICT certification and labelling based on the existing SOG-IS MRA framework. However, an EU-wide certification framework requires more flexibility than is provided by the current SOG-IS MRA. Option 2 would see ENISA function as the secretariat of this new framework, with the agency providing the greater flexibility required by the market by encompassing low to high security assurance models. For instance, ENISA could catalogue certificates and self-assessments and could be also be tasked with monitoring relevant certifications. A new certification framework under ENISA should include more security levels than the current SOG-IS MRA. Moreover, in light of its neutrality vis-à-vis the Member States, the role of managing a labelling scheme for ICT products should be transferred to ENISA once the certification schemes have been approved by the “Board” (option 2) or defined in cooperation with national standardisation bodies (option 3).

As suggested in option 3, the goal is not to transform ENISA into a standardisation body but to ensure closer cooperation in the development of standards which are in line with the defined state-of the art (SOTA) and to identify synergies across IoT verticals. ENISA should be given a well-defined remit and should provide support services such as threat analysis, trusted information exchange and advice on standards and certification practices. Therefore, Eurosmart supports the adoption of a new legislative instrument to support ICT security legislation. This framework and related labelling should be mandatory and common technical security requirements should also be developed for all vertical sectors.

## **3. Eurosmart’s proposal for a European ICT security certification framework**

A solution should avoid any market distortion and seek to consolidate the digital single market. Therefore, Eurosmart encourages the European Commission to take into consideration proposals from the smart security industry. Eurosmart has developed a meta-Scheme approach that draws together pre-existing solutions to ensure a greater level of flexibility which would enable more complex products like motor vehicles or aeroplanes to be

certified. Furthermore, a meta-framework allows for the addition of arbitrary schemes in the future, thus ensuring that the model is not limited to any kind of existing market. Eurosmart is convinced of the benefits afforded by this solution in addressing all security certification levels and urges the European Commission to include this approach in its upcoming proposal for a European ICT security certification and labelling framework.



## **About Eurosmart**

### *About Eurosmart*

*Eurosmart, the Voice of the Smart Security Industry, is an international non-profit association located in Brussels, representing the Smart Security Industry for multisector applications. Founded in 1995, the association is committed to expanding the world's smart secure devices market, developing smart security standards and continuously improving the quality of security applications.*

*Members are manufacturers of smart cards, semiconductors, terminals, equipment for smart cards system integrators, application developers and issuers who work in dedicated working groups (security, electronic identity, communication, marketing). Members are largely involved in research and development projects at European and international levels.*

*Eurosmart members include companies (Gemalto, Giesecke & Devrient, GS TAG, Imprimerie Nationale, Infineon Technologies, Inside Secure, Linxens, Nedcard, NXP Semiconductors, Oberthur, +ID, Real Casa de la Moneda, Safran Identity and Security, Samsung, Sanoia STMicroelectronics, Toshiba and Trusted Objects, Winbond), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC) and associations (Pôle SCS, Smart Payment Association, Mobismart, Danish Biometrics).*

### **Press contact:**

**Pierre-Jean VERRANDO**

Director of operations

Mobile: +32 471 34 59 64

**EUROSMART**

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

[euromart@euromart.com](mailto:euromart@euromart.com)

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