EUROSMART
The Voice of the Digital Security Industry

Eurosmart welcomes the COREPER agreement on the proposal for a Cybersecurity Competence Centre

Eurosmart is committed to developing technical content to improve digital security solutions. Our community of experts who are key members of the European digital security industry have a long track record in supporting European initiatives which strengthen the cyber resilience of the EU. The future European Cybersecurity Competence Centre (ECCC) is a complementary initiative to help protect and enhance the Digital Single Market. The ECCC complements and enhances the steps already taken through the NIS Directive, eIDAS and the Cybersecurity Act. Eurosmart and its members are fully supportive of this new initiative replace and extend the mission of the Cybersecurity Public-Private Partnership that concludes at the end of 2020.

The current Partnership has been a useful starting point to identify and gather actors from the EU cybersecurity value chain. The emergence of new challenges related to Europe's digital autonomy requires new interactions between the European Research and Technical Organisation (RTOs), the European industry and public authorities. The future European Cybersecurity Competence Centre has the potential to take up the challenge and build relationships of trust within the European cybersecurity community.

The previous European cybersecurity initiatives such as NIS Directive, eIDAS, and the Cybersecurity Act have already enabled the creation of dedicated community of experts. The future Centre should rely on the existing ecosystem which actively contributes to maintaining Europe's cyber resilience at the "State of the Art" level. Security is at the heart of Eurosmart membership, the Eurosmart community of experts has a proven record of providing expertise and a fair representation of the European cybersecurity value chain. Such an approach must also be a key concept for the ECCC Community.

In the context of increasing connectivity and reliance on non-EU solutions and technologies, support of the European cybersecurity industry is critical to maintain a high level of trust in the Digital Single Market. This is a critical aspect for digital sovereignty with respect to both citizens and industry.

The European Cybersecurity Competence Centre is a tremendous opportunity to increase consistency between the different European initiatives and legislations within the cybersecurity field. The Centre will help European cybersecurity actors to better use and benefit from the already existing tools such as the European Certification Framework, GDPR guidelines or certification, vulnerability disclosure etc. whilst helping to support the development of security step-up and innovation.

In addition, Eurosmart calls on the European Cybersecurity Competence Centre to support the full European state of the art approach to key digital technologies (KDTs) as identified by the IPCEI Forum.

The European Digital Security Industry recommends tackling below priorities in the framework of a digital autonomy strategy:

- **Cloud Security:** Europe should pay attention to the way data of citizens and of companies are concretely protected when in the cloud. Isolation, segregation, should be properly implemented, in both private and public clouds, and in particular when operated by 3rd parties. Standards and certifications of proper architectures should be strongly encouraged. Also, the deployment of next generation EU framework for PKI infrastructure should bring access to open, trustworthy, affordable and well-recognized PKI infrastructure.

- **HW security, Root of Trust and supply chains:** whatever the IT technology, the security chain most often starts with a first piece of HW that needs to be trusted: The Root of Trust. It is of great importance for its sovereignty that Europe ensures the deployment of Roots of Trust that are under control. The reliability of their supply chain as well the proper management of their credentials is the foundation of trustable solutions.

- **Strong Authentication:** weak authentication factors (e.g. usernames/passwords) are still massively used in 2020 despite well-known threats and intrinsic weaknesses. Europe should boost the deployment of strong identification and authentication solutions relying on standards, in line with eIDAS provisions.

- **Advanced Cryptography:** the research in advanced cryptography techniques with concrete and efficient deployments in mind should be boosted. Homomorphic encryption, multi-party computation, attribute-based encryption, white box cryptography… are promising techniques that should be stimulated through innovative projects and concrete use cases.

- **Cyber Resilient Engineering:** because infrastructures and solutions are becoming more and more complex, there is a strong need for AI to help analyzing threats and potential weaknesses of complex systems. Also, AI and automation will help in managing the growing volumes of threats and in deploying efficient solutions for detection, reaction, and reconfiguration.

All these topics should be strengthened by EU's certification and standardisation efforts, which imply the full involvement of the European cybersecurity value chain. The mastery and the deployment of such technologies, backed by the European Cybersecurity Competence Centre, will significantly increase the EU market share in digital products and services. This will enable a secure, independent and trustworthy Digital Single Market with a strong reliance on the European centre of excellence.

About us

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.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 3635 | mail eurosmart@eurosmart.com