EUROSMART
The Voice of the Digital Security Industry

European Partnership for Smart Networks and Services

Eurosmart's answer to the European Commission's Public consultation

Eurosmart, the voice of the digital security industry, is committed in providing and enhancing security solution to enable European citizens to benefit from reliable and trustworthy digital experience. Infrastructure security and trustworthy services are essential building blocks for the European Cybersecurity policy. Eurosmart welcomes the effort of the European Commission to strengthen the cybersecurity value chain and to give the European industry the opportunity to develop advanced solutions and to increase its know-how for smart networks and their related services.

In defining the connectivity for the future, Europe would be able to shape its own digital autonomy and to make its industry compete on the global stage. The proper management of such key enabling technologies is also a matter of digital sovereignty.

To achieve this goal and to develop the European leadership, the time-to-market for smart connectivity is paramount. Eurosmart enjoins the legislator to define the suitable solution to gather the whole chains for "Industrial Internet of Things" and "Connected, Automated and Electric Vehicles" while focusing on the standardisation activities and in particular with the European Standardisation organisations. An EU strategy is required to define future-proof and quickly implementable solutions.

A European Partnership for the emergence of European global leaders in innovation

Communication systems, secure solutions and networks shall gather forces to define, implement and deploy smart networks and services. The need in R&I to develop smart network for the future is more than significant and should contribute to the definition of a comprehensive EU Cybersecurity digital strategy. This could lead to the emergence of European global leaders in innovation that will be world leaders in their respective fields. This will require focusing investment on competitive advantages for the market uptake of European demand-oriented solutions. For these reasons, Eurosmart supports option 2b: institutionalized partnership based on Article 187 TFEU with the support of the Member States. Meanwhile this option should not lead to a cluster of few involved parties but engage with the whole value-chains for 5G, Interatrial IoT and automotive. Besides, a coordination amongst the member states should be ensured to allow a convergence of the defined projects and strategies.

Eurosmart would like to focus several topics to be tackled to support smart network and services:

Enabling trustworthy 5G connectivity infrastructure and applications

Connected vehicles, (Industrial) Internet of things and (critical) applications require access to resilient wireless network. 5G connectivity infrastructure is the backbone of the future European Digital economy, efforts should be made to support R&I in this field to make Europe master the essential 5G technologies. Eurosmart encourages the Commission to back efforts to ensure the trustworthiness of the 5G system in terms of resilience, security of communications, identity management, privacy and security assurance.

Eurosmart supports the principle of consistent security across the entire 5G architecture, from the core network within the core network and distributed to the edge. This approach necessitates the involvement of the whole 5G value chain and digital security providers in the EU R&I action plan. 5G Network should also prevents malware from being transmitted to connected devices to protect consumers from cyberattacks. Security mechanism should be deployed to prevent unauthorized command-and-control activities, from being exploited by connected devices.

To protect the whole infrastructure, automated threat-discovery mechanisms should be developed and distributed across key points in the core network and at the network edge. This mechanism shall enable rapid identification of infected hosts and a rapid resolution of security-related incidents. In term of prevention, procedures and solutions should be implemented to prevent malware from entering network functions, then spreading through other functions and infecting individual 5G slices.

Following these principles to enable security from the core network to the edge, local or edge connectivity software should be running on a certified hardware. The European Union has made huge efforts to enhance certification mechanisms in cybersecurity, this is a key element to ensure resilience of 5G infrastructure.

The next generation EU framework for PKI infrastructure

PKIs play a key role in establishing trust over the Internet as allow on a side to mutually authenticate parties (human or machines) an on the other, if used correctly, to secure communication channels and data. Today however, many PKI (Public Key Infrastructure) applications are not accepted on the long end, due to the lack of access to open, trustworthy, affordable and well-recognized PKI infrastructure, (i.e. cross-border applications for eHealth, eID, intelligent transport systems, e-government services etc). This is a clear obstacle to the development of a more interoperable and secure digital space.

European root DNS for critical infrastructures

DNS is believed to be extremely robust, however, cyberattacks happened in the recent years (e.g. Mirai attack), demonstrated how its infrastructure is today potentially vulnerable. Moreover, the governance of DNS, since its creation, has been managed by ICANN, a private organisation under the US law. Therefore, the alignment of its governance with the European interests is required to achieve a sufficient security level for internet services. When it comes to critical services, a European root DNS management could be initiated to protect Europe's digital assets.

Develop and deploy end-to-end data protection solutions using advanced cryptography

More generally, R&I should focus on the development and the deployment of advanced cryptographic functions and protocols to secure data transmission over unsecured network. Europe has a strong

background in theoretical and mathematics basis of cryptography, and innovative schemes development should be encouraged, supported and pushed to proof of concept and standardisation. Homomorphic encryption enabling the use of untrusted cloud services, Identity and Attribute based encryption (IBE, ABE) enabling global secure solutions with massively interconnected objects are technologies to support. European commission could, in collaboration with Member States, make available, research and innovation funds for breakthrough and patenting on advanced cryptography. This should comprise also innovative cybersecurity deployment projects, including pilot lines launch calls for proposals for an amount to be defined.

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 manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Renaud**), 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 and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

Contact:

Pierre-Jean VERRANDO
Director General
Mobile: +32 471 34 59 64

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