EUROSMART
The Voice of the Digital Security Industry

European Partnership for Key Digital Technologies (KDTs)

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

Eurosmart is deeply involved in the enhancement of Key Digital Technologies (KDTs) and more precisely in the fields of cybersecurity and digital trust. Our organisation nurtures a world-wide recognised know-how in digital security based on European-based trustworthy solutions. The digital transformation, Internet of Things, Artificial Intelligence, autonomous automotive and 5G are key challenges for the European industry, competition with other economics areas such as China, South-Korea, Japan and the United-States has been increasing over the last decades. For the first time in the History, the so-called digital transformation is the first industrial revolution which was not born in Europe. Even if most of the digital Key enabling technologies has been araised outside the continent, most of them and in particular the cybersecurity ones, have been developed and firstly implemented in Europe.

The complete mastery of KITs is key for the European Industry and their consumers, it is a matter of Industrial policy with the aim of increasing the EU market share of digital product and services in order to become a net exporter. This is also a question of independence and sovereignty, by making product and services even sustainable and more secure according to the expectations of the EU market and based on trustworthy and interoperable European standards.

A joint undertaking to support the European Partnership for KDTs

The key aim of the European Partnership for Key Digital Technologies is to bring together the European fragmented ecosystem for Electronic Components, System community and more generally the European digital manufacturers and service providers. This new European partnership shall leverage on the achievements in terms of governance and projects of the Joint-undertaking on electronics and component systems for European leadership (ECSEL) and shall widen its scope to address the whole European digital value chain.

When it comes to cybersecurity and digital security, which are the core topics of Eurosmart, we recommend to fully implement the priorities identified by the Strategic Forum for Important Projects of Common European Interests (IPCEIs). These recommendations are of overriding importance to make EU as a global leader in key areas of Cybersecurity. European Key Digital Technologies must rely on a holistic and integrated approach to Cybersecurity. Eurosmart strongly believes that Cybersecurity, thanks the unique European know-how in this field, can make Europe compete on the digital global stage.

For these reasons, Eurosmart favours option 3 “institutionalised partnership based on Article 187 TFUE” which would create a joint undertaking (JU) gathering the European Commission, stakeholders and Member States. Industry and stakeholders alongside the Member States and the European Union would be able to jointly address priorities and set up agenda based on the definition of a common European Strategy. This option involving stakeholders in the decision-making process will be able to attract the digital ecosystem and would help the European and national institutions to identify experts from industry and research organisations. This set-up would guarantee the involvement of stakeholders and the relevance of their profile.

Involvement of parties within the expected joint undertaking

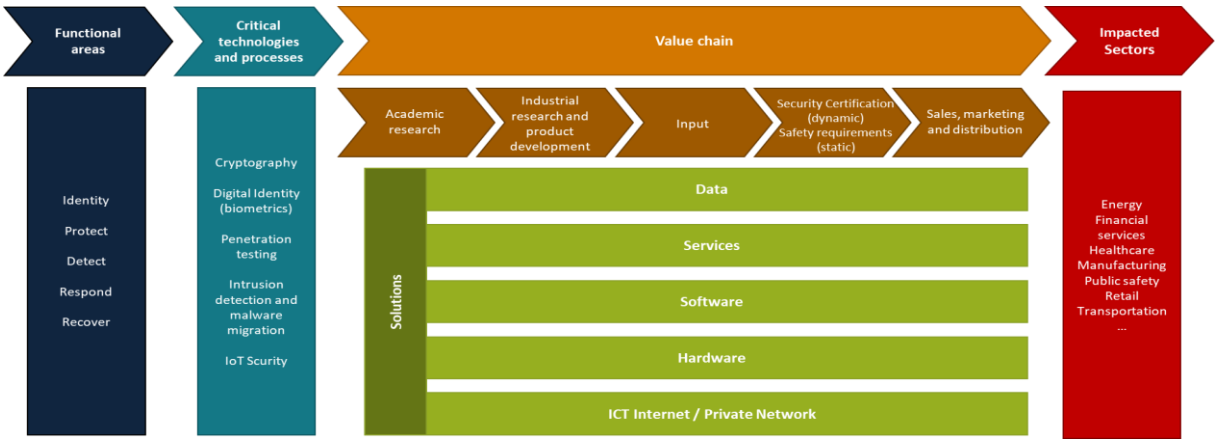
To contribute to the success of such an initiative, Eurosmart recommends reaching a fair balance between the stakeholders represented within the JU. The JU cannot become a privileged area dedicated to few actors which have their say to the Commission and to the Member States and which orientate the strategic objectives to their own private benefits. To avoid such a situation, clear rules should be set up since the establishment of the JU with a fair representativity of the digital ecosystem who share the same European values: industry, research and technology organisations (RTOs), several verticals, academics.

A definition of a Multi Annual Strategic Plan providing a long-term view coupled with a Research Agenda would help to define the goals to be achieved and set up the metrics to analyse potential improvements. These tools would grant sustainability to the work and to the projects undertaken and would contribute to the definition of the European digital industrial strategy.

In addition, since the projects are co-financed by the Member States, the EU Council and the Commission shall take care of the involvement and the Member States and established trusted channels of communications: At the highest political level a discussion should be initiated towards harmonisation and synchronisation of the Member State participation rules.

A particular attention shall be paid to the dissemination, tools and synergies must be developed to facilitate the integration and the reuse of the results of the JU across sectors and verticals. To avoid any overlaps with other initiatives consistency shall be ensured with other European initiatives and actors such as the several Public Private Partnership developed within the Digital Single Market and the European Standardisation organisations.

Within the KDTs, Cybersecurity is playing a major role, the European Partnership for Key Digital Technologies is expected to work closely with the future European Competence Centre and make sure that all its whole value chain is concerned. Eurosmart has identified several digital securitu areas, technologies and actors to support KDTs:



Cybersecurity Priorities for KDTs

As priorities for Cybersecurity KDTs, Eurosmart recommends working on[1]

- **The next generation EU framework for PKI infrastructure and European DNS management for critical infrastructure.** 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.The DNS is instead part of the backbone on which every digital service is built on today. Even if the Internet has no central coordination point, its addressing structure is centrally coordinated through its DNS, roughly speaking a set of hierarchical phonebooks, where names of "online services" are associated with IP numbers.
- **The deployment Shared Database for AI development in cybersecurity.** The adoption of AI and machine learning for security uses are slowed down because it is difficult to access real data and attack data for sensibility reasons. It would be helpful to have a shared database at the European level of attacks and legitimate data (facts, events, network flows, etc.). The shared database could also be composed by different remote databases as in a network of federated databases. The important fact is to have a normalized terminology stored into databases so to improve, to maximize the comprehension and inter communications between final users.
- **The development of homomorphic encryption.** Cryptography is the key technology to secure digital applications. 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 standardization. Homomorphic encryption is the cloud privacy game-changer to come, 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. Homomorphic encryption is a form of encryption that allows correct computation using ciphertexts only without revealing the plaintext.

[1] As part of the Eurosmart's recommendations to the IPCEI

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