EUROSMART
The Voice of the Smart Security Industry

CYBERSECURITY IN EUROPE

TOWARDS AN INDUSTRIAL POLICY

January 2017

CYBERSECURITY IN EUROPE

TOWARDS AN INDUSTRIAL POLICY

Security is a cornerstone when it comes to the protection of data and privacy. Recent cyber-attacks in the US have demonstrated that security by design represents a key objective in politics, for the industry and for citizens. However, for many users convenience is more important than security. This poses a challenge both for policy makers and the Smart Security Industry: combining quick, easy, and fast access to transactions with failsafe security. Trust is crucial for citizens to accept a European digital and mobile economy. The connected society in Europe is also dependent on how secure citizens feel about their digital identity.

Smart Security Industry major economic factor in Europe

Looking at increasingly nationalist protective tendencies in China (program "Made in China"), in India ("Make in India") and the US ("America First"), it is more important than ever that the European Union formulates and represents a strong Digital Single Market policy.

The Smart Security Industry will back the EU in this endeavour and pledges its support for a "Certified in Europe" strategy.

The members of Eurosmart, the Smart Security Industry, including all major European IT companies, represent one of the biggest European industries, driving the European economy in many sectors.

The industry generates an annual turnover of over 15 billion euros, 40% of which is in Europe, and it employs close to 60,000 people worldwide, of whom more than 50% work in the European Union (EU).

Even in times of economic downturn, the Smart Security Industry remains an area for business growth in Europe and worldwide, positively impacting many other business sectors. As we are going towards a hyperconnected society, the Smart Security Industry is essential for the European Union. Hence, there is a need for the establishment of standards in this field.

An industrial policy would set unequivocal standards for security with regards to:

- **Security by design:** security principles such as confidentiality, integrity, and availability must be included as basic requirements in the initial architecture and not as an afterthought in the development cycle. This would also be another step to augmented user convenience as protection would be built in.
- **Privacy by design:** all hardware manufacturers are required to implement data protection already in the hardware so that, by default, the personal data of citizens are protected. The security standards used in privacy by design must be based on tested and proven state-of-the-art certification procedures like CCRA or SOG-IS MRA;
- **A new European trust label:** "Certified in Europe", should be built on defined security requirements and recognised certification schemes. This should provide trust visibility to users and OEMs and allow verification of compliance with privacy by design;
- **Secure element-related security standards:** both European and international, as defined by corresponding bodies such as Global Platform, EMV Co, or FIDO ("Fast IDentity Online") Alliance, is crucial for guaranteeing the security in a EU Digital Single Market.[1]

1 The security levels should balance the implementation complexity/cost and the needed level of protection of data. A well-defined security scheme is key. In the regulation corner the eIDAS EC/910/2014 is a good example for privacy aspects, which defines three security levels. On the technical standardization side the IEC 62443-3-3 for industrial network and system is another example for data protection (confidential and strictly confidential), which describes four security levels and three types of identities for persons, machines and objects.

ECSO crucial platform

Eurosmart, the Voice of the Smart Security Industry in Europe, has been advocating the highest security for digital and mobile solutions in cyberspace since its inception in 1995. The members of Eurosmart offer products and solutions that cover every level of security requirements, from applications that only need an entry level of security, such as loyalty programs, to transactions for which the highest security is indispensable, such as financial or eGovernment applications. Eurosmart therefore welcomes the European Commission's commitment to cybersecurity as a core element of the European Union's Digital Single Market and its willingness to make use of the Smart Security Industry's expertise.

The European Cybersecurity Organisation (ECSO) is the crucial platform for:

- **exchanging ideas defining the EU cyber strategy, the future EU certification scheme for cyber security product and systems and also**
- **for building trust among all market players, and**
- **for shaping the future research along HORIZON 2020 on cybersecurity for the benefit of the European citizens, the European industry and the EU Member States.**

Eurosmart is a founding member of ECSO and pledges its full support for ECSO's objectives and purpose. The Smart Security Industry would – to show the strength of its commitment to the Digital Single Market and a European hyperconnected society – delegate its President to the ECSO Board of Directors, and its Vice President to the Partnership Board.

Industrial policy for a better Digital Single Market

Eurosmart regards the various European activities for standardisation of cybersecurity, such as ECSO, AIOTI Private Public Partnerships, or the EU trust label as a step in the right direction. As in every other area of politics, coordinating national into European activities and establishing standards for European markets is crucial for the success of European political initiatives.

Eurosmart therefore suggests to complement the existing individual EU activities mentioned above with technological standards and to channel all activities into an industrial policy sufficient to achieve the goal of a secure EU Digital Single Market.

Eurosmart understands that in some applications and transactions user convenience outweighs security. This, however, cannot apply to the question of digital identities and sensitive applications such as eGovernment and eFinance. In these fields, using the highest security standards possible is vital. In order to deploy digital services and solutions throughout the Digital Single European Market, it is imperative that technological standards for digital identities, digital signature of persons or physical products are established as baseline for privacy and security by design. Standards guarantee interoperability of systems and technologies and will thus enable a deployment of innovative services and solutions across Europe, with a high level of consumer and personal data protection.

Expand European security certification schemes and policy

The Common Criteria (CC) certification[1] and Baseline Certification (BL) address different security levels and should be consequently used in all EU member states for high security applications as well as for security products

A trust label could help citizens, enterprises and public authorities with the decision in procurement processes. The EU trust seal, used by the Regulation EC/910/2014 since June 2016 for trusted service provider is an example for a trust label in the digital Europe.[2]

Eurosmart as a founding member of the European Cybersecurity Organisation (ECSO) will continue its dialogue with EU decision makers and bring its expertise and experience to this organisation. Eurosmart believes that ECSO, through the consent achieved by its participants, plays a major role in shaping the European policy on cybersecurity and the Digital Single Market, ensuring ICT security and the protection of data and privacy.

1 Associated to the SOGIS Mutual Recognition Agreement.

2 On higher security levels (4 and 3) as defined in IEC 62443, embedded hardware security is needed, to realize the robustness, protection against cyberattacks and to get a CC-certification for web-connected products. For lower security level (2 and 1) an embedded secure anchor is recommend, which has a security certification along CC (ISO/IEC 15408), and which are based on international standards, such as ISO/IEC 11889. Those security anchors should be developed and certified in Europe and can support all relevant security functions such as encryption, key storage, secure communication, secure SW update, secure boot, integrity remote attestation which have no backdoor functionality.

EUROSMART
The Voice of the Smart Security Industry

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 is acknowledged as representing "the Voice of the Smart Security Industry".

For more information, please visit www.eurosmart.com

EUROSMART
Rue du Luxembourg 19-21
B-1000 Brussels

eurosmart@eurosmart.com
Tel.: +32 2 506 88 38
Fax.: +32 2 506 88 25