EUROSMART

The Voice of the Smart Security Industry

Eurosmart Position Paper on the European Commission's proposal for a Regulation on Electronic transactions in the internal market: electronic identification and trust services

March 2013

In our digital society, securing digital information and transactions is an important and growing challenge for governments, businesses and individuals alike. Fostering economic growth in Europe will depend on our capacity to develop innovative solutions that will enhance the usability of digital services while protecting privacy and combating fraud. This in turn depends on deploying robust and secure solutions for electronic authentication and signature. The Digital Agenda for Europe has given a political mandate to the European Commission to establish a clear legal framework to prevent cybercrime, and to eliminate fragmentation and lack of interoperability, while enhancing digital identity.

Eurosmart welcomes the European Commission's proposal for a **regulation on eIdentification, eAuthentication and eSignatures** and Trusted **Services** (eIDAS) as another step forward towards removing existing barriers to Europe's digital development on the way to the single European Market. **For us, a regulation is better than a directive,** since there is a real need for standardizing the solutions in terms of security, interoperability and privacy protection.

HOWEVER, WE WOULD LIKE TO STRESS FOUR MAIN POINTS WE BELIEVE SHOULD BE INCLUDED WITHIN THE PROPOSED eIDAS REGULATION:

Point 1: **Protecting personal data is part of the Charter of Fundamental Rights of the EU, and online privacy has always been a cornerstone of the use of the Internet in Europe**. Hence, so as to be fully supported and endorsed by all stakeholders, we highlight that:

- The regulation should include an **article requesting the use of privacy protection mechanisms.**
- When Directive 95/46/EC is mentioned in Article 11, regarding Trust Service providers (and supervisory bodies) , "**Processing of personal data" should imply both the protection of personal data in databases and the leakage of data that may allow tracing back to the user.**

The text should guarantee the right for **online authentication with anonymity**. This would also be an important provision for the proposal for a new legal framework for the protection of personal data in the EU.

Eurosmart proposal #1:

We call for the **introduction of a provision allowing for anonymous Internet identification and authentication** in the proposed regulation**.** This provision will allow European e-services providers to make use of strong authentication without requesting non-necessary personal data to complete transactions on the Internet (subject for instance only to age verification).

Furthermore, we suggest this anonymous Internet identification and authentication is secured by a portable smart secure devices. In our experience, citizens are more apt to put their trust in a secure, portable and personal object. It acts like a "safety deposit box", containing their personal data and rights, protected by strong authentication based on "what I have" (my smart secure device) and "what I know" (the PIN code or password). The use of the personal device is an **unambiguous voluntary act**, and a key opportunity to guarantee anonymous internet identification and authentication.

Point 2: Eurosmart **does not support the use of 16 delegated acts in 42 paragraphs** that will delegate the introduction of applicable standards for the proposed eIDAS regulation. From our point of view, strong efforts have been made and all necessary standards have already been created by European Standardisation Organisations – European Committee for Standardization (CEN) and European Telecommunications Standards Institute (ETSI) - which have been funded by the EU for many years. ISO standards can also be used when necessary.

Eurosmart proposal #2:

We propose **including existing standards in the Regulation, rather than making extensive references to delegated acts**. Such standards would not foreclose future technological solutions as the references can **be amended, removed or replaced** through **implementing acts** once the proposed regulation is in force. At the same time, mandating yet-to-be-written standards would impose **unacceptable pressure on the standards production process**, as well as delegating excessive regulatory power to the technical level.

For security related requirements, existing standards for electronic signatures should be referenced in the corpus of the proposed regulation. ISO work is widely used in several European specifications from the CEN and ETSI, in particular to provide definitions for security mechanisms such as identification and authentication (see ISO 7498) or padding (see ISO 9798, 9796) or data protection and security features such as privacy, anonymity, unlinkability (see ISO 15408) or for smart card APDU commands (ISO 7816).

We would like to highlight that the overall level of security will be determined by the weaker identification system notified. The requirement of a minimum security standard should be the key of the regulation. A possible classification of such security standards was made in the EU ICT Large Scale Pilot Project STORK.

For interoperability concerns, we recommend that prior to the obligation to acknowledge a notified identification system, the interoperability evidence should be demonstrated. Regarding Electronic Signature infrastructure, we recommend referencing the existing ETSI standards.

The ETSI Electronic Signature group (ESI) has established a harmonised infrastructure for electronic signatures, including conformity assessment, testing compliance and interoperability. The working group is addressing:

- Advanced electronic signatures (XAdES, CAdES, PAdES)
- Signature policies (and XML/ASN.1 format)
- Policy, security requirements and profiles for Trusted Service Providers issuing certificates, for TSP providing TS, signature generation and signature validation services
- Services such as registered email (REM), data preservation
- Trust service status lists providers (format)
- And signature suites

Regarding Qualified Secure Signature Creation Device (SSCD), we recommend referencing the existing CEN-Standard Technical Committee 224 (Machine-readable cards, related device interfaces and operations) which is developing inter-industry standards for secure elements and related interfaces, personal identification including authentication and confidentiality, electronic signature and SSCD life management. Several working groups are in charge of electronic signature standardisation:

- CEN TC 224 WG16 is developing and maintaining EN 14890, where SSCD requirements are described as producing a "qualified electronic signature" and supporting the concrete implementation of the European legal framework for electronic signatures, to be the base standard for personalised cards with e-IAS services, in order to enable the development of interoperable applications.

- CEN TC 224 WG17 is delivering protection profiles linked to electronic signature: EN 14169 (PP SSCD) for a secure signature creation device, TS 14167 (PP for trustworthy systems managing certificates for electronic signatures) and some new documents for Device Authentication, Signature Creation/Verification Application. The group is also working on server signing functionality (first draft for security requirements is available, see 14167-5, establishment of PP is currently being discussed).

- CEN TC 224 WG15 is delivering European Citizen Card specifications (TS 15480), including in Part 4 national applicative profiles (ID card, signature card, electronic services card). This standard provides a good description of the legacy infrastructures available in different Member States and also allows system integrators, software editors and service providers to use the existing SSCD.

These series of standards are also allowing the use of the Mobile infrastructure such as Mobile phones (and not only smartphones), Tablets and Laptop PCs to run the eIAS application with the same level of security, interoperability and convenience.

Point 3: **Certification of the qualified electronic signature creation devices** is the guarantee that the devices are secure with a level of assurance commensurate with the legal effect of the qualified electronic signature for the user.

The **security evaluation process must be carried out by licensed laboratories** following a standard methodology that is well adapted and tested for this kind of device. The security assessment must include an assessment of a high resistance to attacks, for which the level must be unambiguous, homogeneous between laboratories and maintained at the state of the art of the attacks.

Recognition of the certificates must be based on the mutual recognition of the certification bodies as capable of delivering these certificates. The SOGIS Mutual Recognition Agreement (Council decision 92/142/ECC and Council recommendation 95/144/EC) successfully built a framework for coordinated security evaluation and certification of such devices. Its proven and available expertise should be a reference.

Eurosmart proposal #3:

We call for a **mandatory certification of the qualified electronic signature creation devices**. Rather than deferring to implementing acts to be adopted at a later stage, we recommend adopting the **ISO 15408 standard** (Common Criteria for IT security evaluation) applied in the context of a mutual recognition agreement such as SOGIS MRA or built on it.

Point 4: The proposed eIDAS regulation has a **major impact on all members of the European Smart Security industry.** This industry, with its European roots, has developed worldwide for more than 20 years to a point where Eurosmart has reported that over **7 billion smart secure devices were shipped in 2012**. All its leaders are based in the European Union, with more than 50% of their headcount in the EU. Today, the 17 industrial members of Eurosmart have a total annual turnover of over €60Bn.

Thanks to the development of international standards by the European standardisation bodies and European industry, smart secure devices have contributed to the development of mobile telephony (SIMs), secure payments (EMV banking card), eIdentity (ePassports, biometric Passports, tachographs, eResident permits, eID cards, eDriving licences, eHealthcare cards, eVoting cards) and solutions for eBanking and eCommerce (smart secure tokens, EMV card readers). Huge investments have been made by the EU and the Member States to support this dynamic and massively exporting industry.

Yet one of the main challenges of the digital world is to foster security and trust for Internet based services. Several electronic identification initiatives exist, notably in Europe, but also in the United States. We believe that the US will leverage **their successful experience** in using the secure element to provide trusted digital identity in Cyberspace as they have done for **all federal employees and contractors**. The Homeland Security Presidential Directive-12, "Policies for a Common Identification Standard for Federal Employees and Contractors," requires implementation of a mandatory, government-wide standard for secure and reliable forms of smart card identification for federal employees and contractors requiring logical access to federally controlled information systems.

Eurosmart would like to emphasise that **the complete secure element sub-system in the United States is delivered by European companies**. This demonstrates the advance of European companies in the Digital Security field.

Eurosmart proposal #4:

We are convinced that Europe has a great opportunity to federate existing electronic identification initiatives by creating a global and unique electronic identification, authentication and signature standard. We believe that **the current discussions should take into account any provisions related to interoperability with the future USA scheme – the NTSIC program: National Strategy for Trusted Identities in the Cyberspace**.

The Internet has no borders, and from a Eurosmart perspective, the **online world should remain borderless** while protecting any citizen regardless of his country of origin or that of his/her service provider.

The proposed regulation for electronic identification and trust services sets an ambitious goal for the **development of the European Single Digital market**. Reliable electronic identification trusted by the European citizen and embedded in a portable, smart secure device with privacy-by-design is key for fostering growth of the digital economy.

For the smart security industry, for identity providers and secure service providers in the digital world, reliable planning is needed. With the approach of the 16 delegated acts this reliable planning would be very difficult. If 27 different identification schemes were to be notified in Europe, a Belgian service provider would for instance have to support 27 different identification systems, meaning different data sets, different authentications schemes (e.g. one-factor, two factor authentication), different authentication protocols and different security architectures. If a delegated act changes over the time any legal aspects, which generate a need for a technical change, the service provider would have to budget additional financial resources.

Eurosmart's experts are ready to assist the European Commission, the Members of the European Parliament as well as the Member States in reaching this important objective for Europe.

EUROSMART

The Voice of the Smart Security Industry

About Eurosmart

Eurosmart is an international non-profit association located in Brussels and 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 the European and international levels.

Eurosmart members are companies (Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Infineon Technologies, Inside Secure, LFoundry, Morpho, NedCard, NXP Semiconductors, Oberthur Technologies, Prooftag, Renesas Electronics, Samsung, STMicroelectronics, Toshiba), payment systems (GIE Cartes Bancaires, Mastercard), laboratories (CEALETI), research organisations (Fraunhofer AISEC), associations (Smart Payment Association, Mobismart, Danish Biometrics) and independent experts (Michel Koenig, Jonas Andersson).

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

For more information, please visit www.eurosmart.com

Contact:
Oyvind Rastad
Eurosmart Chairman
Rue du Luxembourg 19-21
B-1000 Brussels
Belgium
eurosmart@eurosmart.com
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25