POSITION PAPER

DIGITAL IDENTITY SECURITY:

SOGIS-MRA AS A COMMON FRAMEWORK TOWARDS DIGITAL TRUST

SUMMARY AND RECOMMENDATIONS:

The concept of digital identity is tightly linked to personal data protection and privacy protection. In connection to the level of assurance of the identity, the intrinsic security of the solution is essential – Eurosmart works with and makes proposals on all these issues. The present document makes a statement on the security that shall be applied to electronic identification in the context of the regulation of electronic identification and trust services for electronic transactions in the internal market (so-called eIDAS Regulation).

The ISO/IEC standards and the STORK European project have defined four levels of digital identity assurance (*minimal, low, substantial and high*).

For Eurosmart, a "high" level must:
- Guarantee that the digital identity presented matches the true identity of the connected individual;
- Be based on secure solutions that have been evaluated and certified in compliance with a proven methodology.

These 2 objectives are mingled, and a provable identity requires a trusted solution.

For transactions where a security breach could cause severe damage, Eurosmart recommends to use a high level of assurance, based on a "secure element". A secure element is a personal portable object that remains under the holder's sole control, and the best way to counter security vulnerabilities. They are designed, evaluated and certified according to are designed, evaluated and certified according to the Common Criteria and their certificates are recognized by the SOGIS-MRA for both hardware and software.

SOGIS-MRA was set up and signed by 10 European Member States and targets mutual recognition up to the highest levels of security; is open to EU and EFTA Member States who can be either consumers or issuers of certificates.

In order to bring trust and successfully achieve the goals of the eIDAS Regulation, Eurosmart recommends:
1 – The deployment in Europe of a "high assurance" level for digital identities, security certified in reference to SOGIS-MRA
2 – The support and the enlargement of SOGIS-MRA as a common framework and a strong basis for intergovernmental cooperation towards a more secure environment for digital identities.

Evaluation and certification:

ISO/IEC 15408 has published the set of standards known as "Common Criteria" for the impartial evaluation of IT systems and software. CCRA sets the mutual recognition agreements that warrant the acceptance of the security certificates delivered by the countries that are the signatories of the agreements.

Common Criteria provides guidelines for the development and security checking of products and systems that deal with personal data. It sets a methodology for both the developer of the solution and the evaluation officer. Functional requirements for security and security assurance needs are described. A certificate is issued by an authority in charge of the certification, taking into account the conclusions of the evaluation report. This certificate guarantees that the evaluated product or technology complies with a level of assurance ranging from EAL1 to EAL7[1]. A set of minimal assurance requirements corresponds to each level.

Protection Profiles (PP) define the security requirements for a category of products, taking into consideration their use (for instance travel document, electronic signature, etc.) and not their implementation.

Common Criteria allows:

- End users to define their security policy and judge whether a product fulfills their needs in terms of security
- Developers to identify the security requirements that the product must fulfill
- Evaluation officers to verify that a product complies with its evaluation target, according to a methodology and standardized criteria.

A key point of Common Criteria is the examination of resistance to attacks made in view of compromising security and, in particular, access to data. The vulnerability analysis is materialized by a grade from AVA_VAN.1 to AVA_VAN.5[2]. A more advanced study is indicated by the "+" sign after the allocated EAL quotation; however, it is relevant to verify in the certificate that this "+" sign is really relative to vulnerability robustness. Evaluation laboratories have the obligation to employ experts, to have on-going technology surveys, to maintain very good knowledge of the attacks and to proceed to attacks on the products using sophisticated means. This guarantees a high level of resistance of products against powerful attacks. Before proceeding to attacks, the laboratories must have perfect knowledge of the design of the products, including the software source code.

Two agreements for mutual recognition of Common Criteria certificates have been concluded:

- CCRA, which gathers 17 signatory countries and 9 other countries that officially recognize the certificates. By this agreement, mutual recognition is limited to the EAL2 level (or EAL4 under certain conditions)
- SOGIS-MRA was set up and signed by 1O EU Member States and targets mutual recognition up to the highest levels of security (up to EAL7 and AVA_VAN5).

Other security evaluation methods have been published, but have not yet given birth to mutual recognition agreements.

[1] EAL : Evaluation Assurance Level
[2] AVA: Vulnerability assessment class _ VAN : Vulnerability Analysis

Eurosmart's position

Eurosmart is willing to contribute to the creation of a world of digital trust for all stakeholders. Common Criteria and, more particularly, the SOGIS-MRA agreement will enable achievement of this goal.

A digital identity with a high level of assurance shall be used in transactions where a security breach could cause severe damage. Eurosmart recommends the use of a "secure element" supporting the digital identity. A secure element is a personal portable object that remains under the holder's sole control. The interest in attacks is insignificant compared to the appeal of databases containing high volumes of personal data. A secure element is a system in which communication means are restricted and in which security is easier to control. Secure elements are designed, evaluated and certified according to Common Criteria and their certificates are recognized by SOGIS-MRA for both hardware and software. Developers, evaluation officers and certification officers have a very high level of expertise.

Applying a security policy from the start of development drastically reduces the security vulnerabilities and thus the risks of security breach. The expertise achieved is extremely important with respect to the robustness against high-level attacks. It allows defining the legal basis of the liability of the actors in cases of fraud, security breaches and damages to repair.

Of course, security has a cost. Development of security evaluated and certified technology takes more time and money, but these are mainly fixed costs that become small when related to units sold. Also, these costs have to be compared to the severe risks for individuals, enterprises and the whole economy.

Secure element technology is now at the core of a widespread, worldwide ecosystem. The huge number of certificates issued annually is a testimony to the vitality of the system.

SOGIS-MRA is open to EU and EFTA Member States who can be either consumers or issuers of certificates. They work together on the development and survey of the system. For instance, certification officers are audited by their peers. Nowadays, international Requests for Proposals are proof of the de facto recognition of SOGIS-MRA.

Eurosmart's hope is that SOGIS-MRA will become better known and understood in order to allow more Member States to participate.

In this view, Eurosmart recommends:

1 – The deployment in Europe of a "high assurance" level for digital identities, security certified in reference to SOGIS-MRA;
2 – The support and the enlargement of SOGIS-MRA as a common framework and a strong basis for intergovernmental cooperation towards a more secure environment for digital identities.

This is a key matter for the protection of the European citizens' digital identities, and Eurosmart's experts remain at the full disposal of the European Commission to provide additional information, share their expertise and work with the Member States and other relevant bodies.

About Eurosmart

Eurosmart is an international non-profit organization located in Brussels which represents the Smart Security Industry for multi-sector applications. Since its creation1995, the association has been committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services for various market segments – telecoms, financial services, government, healthcare, transport, etc. Its Electronic Identity working group has published many papers and contributions for all applications relative to identity.

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, mobile trust, communication, and marketing).

Members are largely involved in research and development projects at the European and international levels.

Eurosmart members are companies (Athena Smartcard, Austria Card, EM Electronic Marin, FNMT-RCM, Gemalto, Giesecke & Devrient, Imprimerie Nationale, Infineon Technologies, Inside Secure, LFoundry, Linxens, Morpho, Microsoft, NedCard, NXP Semiconductors, Oberthur Technologies, Samsung, STMicroelectronics, Toshiba), payment systems (Mastercard), laboratories (CEA-LETI), 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:
Didier Sallé
General Secretary
Rue du Luxembourg 19-21
B-1000 Brussels
Belgium
didier.sallé@eurosmart.com
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25