A Trusted Digital Identity: a Fundamental Right for all European Citizens

Recommendations by the Smart Security Industry on security assurance levels and qualified electronic signature

Digital trust is at the heart of a functioning hyperconnected society, especially where eGovernment services are offered. The key to digital trust is a secure and protected digital identity. Citizens have a right to expect their governments to enable the use of a trusted digital identity by implementing the highest security standards possible. Vice versa, Governments have the obligation to protect their citizens' digital identity by ensuring the privacy and security of the data in question.

- The eIDAS Implementing Act defining **security assurance levels** must therefore define the level of assurance for the security certification as "High" (the highest level possible) in compliance with the SOGIS-MRA, at level EAL4+, including the AVA_VAN 5 resistance to high level attacks. The level of assurance "high" must also apply both for all modes of electronic identification and of authentication.

- In the delegated act relating to the **qualified electronic signature**, whether performed via server or with a personal device, the level of assurance must also be defined as"high" for all modes of electronic identification and authentication.

Safeguarding the privacy and personal data of EU citizens

The means to safeguard trusted digital identities have been made available both on political and technological levels. In 1992, the first Senior Officers Group for Information Systems (SOGIS) agreement was produced in response to the EU Council Decision of March 31st 1992 in the field of security of information systems and on common information technology security evaluation criteria. It was later amended to SOGIS MRA (Mutual Recognition Agreement), seeking to establish interoperable digital security standards, that are acknowledged and functional across Europe. Today's security certifications for reliably secure electronic transactions are based on SOGIS MRA and AVA_VAN 5. **The certification at level EAL4+, including AVA_VAN5, is in use in many deployed eID schemes and accepted throughout the EU and worldwide as the model ensuring the highest security**. It has been the key enabler for the development of telecom, payment, healthcare, strong authentication application, as well as identity and travel documents.

Secure authentication and electronic identification are the prerequisites for citizens' peace of mind and freedom of digital movement when performing electronic transactions. When personal data or company assets are part of the information exchanged, any transaction should commence with the identification/authentication of both parties, valid for the session. **It is therefore imperative that adequate security measures be implemented in the corresponding EU and national legislation when it comes to digital identities**.

By proposing the eIDAS regulation the European Commission has done exactly that: creating a legal definition of electronic identification and authentication for the approximately 500 million European citizens. However, **there is one major drawback to the eIDAS legislation: it does not make the highest security standard mandatory. The highest standard of security is certification at level EAL4+, including AVA_VAN5, successfully used in the European Union and worldwide**. Instead, the eIDAS legislation would allow EU member states to issue and use for public services three "Levels of Assurance" (LoA) with

regard to digital identities, without specifying their relative benefits and liabilities. The difference between these three LoA remains unclear, even when it comes to the two highest levels, "substantial" and "high".

Hazards of Lax Security Requirements

A European legislation must not be modelled on a lax way of handling digital identities. **The highest level of security technologically available for digital transactions must be made legally mandatory, so that citizens and service providers can demand the implementation of the highest standards of security to ensure security and protection of data and privacy**. In view of the rising number of hacks and security breaches, every other option is inacceptable.

In 2014, more than one billion data records (electronic identification and authentication using login/password) were breached, in over 1500 breach incidents, an increase of 78% from 2013. **54% of the breaches in 2014 involved identity theft, when in 2013 the breaches mainly concerned financial information. Europe accounted for 12% of the breaches**. In addition, the UK being the only member state publishing detailed statistics, accounts for 60% of all breaches in Europe. All business sectors are impacted by this: retail, financel but also governments, healthcare and technology[1].

Every single incident causes damage to the individuals involved, legally, financially, and even psychologically as the trust in using eServices is undermined. Service providers bear the costs of fraud, costs for damages, loss of intellectual property, loss of trust and reputation.

The Rationale behind high-level security

The numbers of hacks, identity thefts and fraudulent transactions will continue to rise, as will the amount of malicious mobile apps and mobile malware code, corrupting the smartphones and tablets of unsuspecting users. Personal data are much better protected when they are stored in a personal device with secure access protocols, instead of a database that represents a valuable target for attackers. **For the sake of European citizens, it is therefore completely inacceptable to issue a legislation that does not specify the highest security as the standard to be implemented with the level of assurance "high".** For instance, only a trusted digital identity, verified and authenticated by the highest security standards, can ensure the validity of qualified electronic signatures.

Any level of assurance other than "high" in the legislation relating to digital identities and digital transactions would also raise legal questions: who will be held accountable if massive identity thefts and frauds occur because of insufficient security, allowed by EU legislation?

Last but not least, **lowering security for ordinary citizens' digital transactions and identities will have a long-term negative economic impact**. Internet services are part of everyone's daily lives; the digital world has created a thriving economy all of its own, accounting for a considerable amount of new jobs every year. However, this digital economy will only continue to thrive if citizens keep making use of virtual services, such as accessing bank accounts or administrative files, subscription sites, medical files, online gambling sites, the employer's IT network, etc. Once this stops,because the risk of becoming a victim of identity theft or fraud has become too high, a whole section of the world economy will suffer as well.

About Eurosmart

Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector 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. The Smart Security Industry represented by Eurosmart's members has an annual turnover of over €10Bn of which around 40% is made in Europe. It employs close to 60,000 people worldwide, of which more than 50% works in Europe.

Contact

Didier Chaudun
eIDAS Task Force Director
www.eurosmart.com
info@eurosmart.com

Rue du Luxembourg 19-21
B-1000 Brussels, Belgium
Tel: + 32 2 506 88 38
Fax: + 32 2 506 88 25

[1] *All facts and figures from this paragraph were extracted from the Breach Level Index (2014 Annual Report)*