On the application of eIDAS Regulation

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

Eurosmart, the voice of the digital security industry, is committed to providing and enhancing security solution to enable European citizens to benefit from reliable and trustworthy digital experience. The eIDAS regulation has fulfilled its promises. The common definition of "electronic identification" and "electronic authentication" are substantial elements for the enhancement of the digital identity in Europe.

On eID deployment

This eIDAS approach for the digital identity is a combination of electronic identification (answering the "Who I am" question) and electronic authentication (answering the "How to prove who I am" question). This shared approach allows the Member States to define the implementation of specificities.

10 Member States have already notified their eID Schemes for level "High" to the European Commission, and the related information has been published in the EU's Official Journal. Many other eID schemes have been pre-notified. This trend demonstrates the high level of confidence and attests the European excellence for digital identity.

Back to the early stage of consumer devices' revolution, eIDAS was the very first EU regulation to come alongside the massive smartphone deployment. This regulation enacts the European principles of privacy and fundamental values. Personal data are highly valuable and should be protected when they are shared with third-parties in return for a private Digital Identity.

This regulation has highlighted the need for qualitative detection mechanisms for identity spoofing. It has also raised the notion of KYC, which has been implemented in many other regulations such as PSD2. Today, digital identity and privacy are priorities to make the European values fit the digital age, and future European initiatives will encompass the question of Trustworthy AI. Moreover, facial and voice recognition are gaining importance for enabling Digital Identities.

It is necessary to anticipate and size the risks of the use of such technologies. Eurosmart recommends performing mandatory penetration testing to assess biometric technologies, as required by ISO IEC 30107 standards on presentation attack detection.

	1st Notification	High	Substantial	Low
Austria				
Belgium	27 Dec 2018	X		
Bulgaria				
Croatia	07 Nov 2018	X		
Cyprus				
Czechia	13 Sep 2019	X		
Denmark				
Estonia	07 Nov 2018	X		
Finland				
France				
Germany	26 Sep 2017	X		
Greece				
Hungary				
Ireland				
Italy	10 Sep 2018	X	X	X
Latvia				
Lithuania				
Luxembourg	07 Nov 2018	X		
Malta				
Netherlands	13 Sep 2019	X	X	
Poland				
Portugal	28 Feb 2018	X		
Romania				
Slovakia				
Slovenia				
Spain	07 Nov 2018	X		
Sweden				
United Kingdom	02 May 2019		X	X
Nomber of Countries		10	3	2

Fig.1 eID Schemes notified in Europe

Trust services

Amongst the electronic services provided by Trust Services Providers (TSPs) and covered by the eIDAS Regulation, the question of website authentication is expected to become a mechanism extensively used. EU Qualified website authentication certificates (QWAC) is more than a technical matter; it is a question of confidence and strategic autonomy over the internet. QWAC should be the prerequisite for the EU online trust. This approach deserves to be enhanced by strengthening the work of the European Standardisation Organisations (ESOs) towards international industry-led web standards. Both the European Commission, the Member States and ESOs should overcome the reluctance of W3C and world-class internet browser to integrate the use of such EU certificates. This lack of recognition deters users and organisation from investing QWAC. Moreover, QWAC should be the basis for PSD2 web certificates.

Besides, the eIDAS model of trust services deserves to be promoted to secure breeder documents which are the basis for the creation of official national ID documents.

eIDAS CABs accreditation

The eIDAS Regulation introduces a legal framework and establishes a scheme for granting qualified status to these new types of trust services aiming to enhance consumer's trust in the digital environment and to improve the transparency of the trust services market. Trust is fundamental to achieve the European Digital Single Market.

Eurosmart enjoins the European Commission to adopt a clear and formal harmonisation conformity assessment scheme against which the CABs would be accredited by a NAB. This scheme should be based on ETSI EN 319 403 by a NAB, and to being pushed in the international context. This scheme would give more clarity on how qualified trust service providers (QTSP) are assessed. ENISA[1] points out the need to starts this process by involving EA, ETSI, EC, ENISA, ESOs. Eurosmart shares ENISA's mindset and recommends as it follows:

- A centralised list of all CABs indicated whether a CAB has been accredited;
- ENISA, ETSI and CEN to develop and publish a comprehensive set of auditors' requirements;
- ETSI ESI to provide further specifications in the detailing of the requirements for TSP procedures and audit best practice to "set up New Roots" and "CA Key Generation »;
- To improve the visibility and the acceptance of the EU trust mark that could be displayed on websites;
- To grow the value of QWACs outside the EU Digital Single Market by convincing the browsers and OS vendors to include the TSL in their respective root stores;
- Following the same idea, to further investigate PSD2 by offering browser plug-ins for enhanced security.

A delegated act for PP QSCD in the cloud

Eurosmart supports the option of a delegated act for PP QSCD in the cloud as recommended by ENISA[2]. ENISA supports two major CEN standards:

- CEN standards (CEN EN 419 241-2 (Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing dated 2018-05-11) and;
- CEN EN 419 221-5:2018 (Protection Profiles for TSP Cryptographic Modules - Part 5 - Cryptographic Module for Trust Services)).

CEN TC224 has issued both documents which cover the way the TSPs manages signature creation data on behalf of the user as well as on their own behalf. Eurosmart agrees to go beyond the simple supervision of QTSPs since the QSCD certification. When the QSCD is managed on behalf of the signer, the certification could not be limited the crypto-module only. The operational environment should be covered as well since the QSCD handles the signature creation and its related data.

When it come to the cloud signature, the CEN Protection Profile for QSCD for Server Signing, covers the server part. However, this Protection Profile is not referenced into the ANNEX II of the eIDAS regulation. This lack of legal recognition has led to alternative national certification schemes. Member States have issued such schemes to fulfil the gap, but have created market fragmentation. An harmonisation is needed for the electronic signature.

Server signing is a valuable achievement to deploy QSCD it enables a new business model. This new approach charges the costs of the certificate to the economic actor who needs it to perform an online contractual and/or a commercial operation, instead of the holder of the local signature tool.

Enhancement of Implementing Regulation

The advent of disruptive technologies sets up a new distributed framework and architecture for the verification of digital identity of a natural or legal person. Such identity being delivered by several

[1] ENISA, Towards global acceptance of eIDAS audits, January 15, 2019.
https://www.enisa.europa.eu/publications/towards-global-acceptance-of-eidas-audits

[2] ENISA, Assessment of Standards related to eIDAS, December 14, 2018.
https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas

attribute providers, leads to the conclusion that eIDAS identification scheme lacks some information. For instance the multi-issuer, multi-verifier and multi-relying party-based ecosystem allowing for decentralized identity verification, requires an enhanced definition of personal attributes whereas the Annex on Requirements concerning the minimum set of person identification data uniquely representing a natural or a legal person, referred to in Article 11, is too restrictive (COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501).

The given definition does not encompass the variety of verifiable credentials, identity tokens and other certified assertions that are handled by decentralised identity documents on a blockchain and by users and verifiers trusting such blockchain. Besides, the recently created CEN/CENELEC TC on Blockchain and DLT will soon set about working on a Technical Specification on eIDAS/eID compliance, to enable compliance with eIDAS regulation eID requirements, and this TC pay a special attention on interoperability and regulatory issues, notably compliance of blockchain implementations with EU legislations (such as GDPR, eIDAS, NIS...).

Therefore, a delegated act to specify the definition of personal attributes seems necessary to allow in the foreseeable future blockchain-based identification systems to get notified and to claim some LoA.

Conclusions

The recommendations supported by Eurosmart do not require any recast of the eIDAS regulation. The approach adopted deserves enough time to harmonise national models fully. eIDAS as a valuable milestone of the European Digital Single Market, would benefit from technical optimisations which could be translated into delegated acts and necessary European standards.

Amongst the elements to be improved, Eurosmart has identified the following priorities:

- Standardisation and harmonisation by creating a conformity assessment scheme based on ETSI EN 319 403
- Organisational by enabling a peer-review system for CABs, ENISA can be the peer-review organisation.
- Influence by enhancing eIDAS' solutions towards W3C through the ESOs and the European Commission. In addition to this, to request the web browser providers to integrate QWAC.

Diplomatic by promoting the eIDAS model towards EU's partners (Japan, South Korea, US, Brazil, Canada, Africa, Middle East and Latin America).

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**, **G+D Mobile Security**, **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**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **Trust CB**, **WISekey**, **Winbond**), laboratories (**Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Reynaud**), 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