On the application of the eIDAS Regulation

Eurosmart's working document

13/03/2020

Eurosmart, the voice of the Digital Security Industry, is committed to enhancing security solutions that enable European citizens to enjoy a reliable and trustworthy digital experience. eIDAS is a valuable milestone in this respect, as (1) it provides a common basis for electronic identities and (2) ensures that trust services appropriately fulfil their missions.

However, the Digital Single Market has not fully reaped the benefits from the eIDAS Regulation, due to an incomplete implementation across Europe, the persistence of diverging national rules and missing elements in the legislation -especially in the implementing acts. In addition, the eIDAS model of trust services deserves to be promoted to secure breeder documents which are the basis for the creation of official national identity documents.

Executive summary

The recommendations supported by Eurosmart do not require a recast of the eIDAS Regulation. First, it is necessary to effectively implement the legislation. On the other hand, **eIDAS would benefit from technical optimisations** which could be translated into delegated acts and European standards.

Eurosmart recommends to:

- Foster the deployment of eID schemes by (1) ensuring a **common interpretation of the requirements for notification** and (2) guaranteeing an **effective mutual recognition;**
- **Supplement the data sets for natural and legal persons with additional attributes** that could support the development of cross-border services and decentralised provision of identity attributes (review of Implementing Regulation 2015/1501);
- **Broaden the scope of eIDAS to encompass privacy preserving use cases** that could rely on electronic attestation and blockchain technology;
- **Refine the technical specifications and procedures relating to eID assurance levels** to avoid market fragmentation (in relation to Implementing Regulation 2015/1502);
- Strenghten security by performing **penetration testing for biometrics technologies**;
- Allow Member States to **suspend recognition of vulnerable eID means**;
- **Harmonise the technical criteria for qualified trust services;**
- **Harmonise the accreditation process for Conformity Assessment Bodies;**
- Propose a **EU qualified website authentication certificate**;
- Adopt a delegated act for a **Protection Profile for Qualified Signature Creation Devices (QSCD)** in the cloud.

Table of contents

Part I: Electronic identification

On the deployment of eID schemes

A majority of Member States has already embraced the eIDAS Regulation. Twelve Member States have notified their electronic identity (eID) schemes for level "High" to the European Commission, and the related information has been published in the EU Official Journal. Many other eID schemes have been pre-notified. This trend attests the European excellence for digital identity. It also demonstrates that Member States are determined to provide their citizens with a highly reliable eID.

However, the deployment of eID schemes could be hampered by a diverging interpretation of the conditions for notification of an eID scheme, as laid down in Article 7 of eIDAS. It is paramount that all Member States share the same analysis of the conformity of an eID scheme with the points (a) to (f) of this article. It would be detrimental for the global trust, interoperability and, ultimately, widespread use of electronic identity, if an eID scheme were to be notified by a Member State while other Member State(s) disagree(s) with its conformity with such requirements.

> Proposal
>
> The conformity of a proposed eID scheme with each of the criteria defined in Article 7 should be confirmed by the cooperation group.
>
> Such a confirmation should be required prior to any notification of an eID scheme.

Towards an effective recognition of eID schemes

The state of play of eID in Europe currently shows that the notification of an eID scheme does not imply that other Member States have the obligation to (1) interconnect with it, and (2) make it usable for accessing their public services.

As such, this conflicts with the principles enacted in article 6(1) (mutual recognition) mandating mandatory recognition of notified eID schemes with a level of assurance (LoA) "Substantial" or "High" matching the required level of assurance for accessing public services. Pursuant to eIDAS, "such recognition shall take place no more than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph".

In Eurosmart's views, there is no legal ground for this interpretation sorting out theoretical recognition (notification of eID scheme) and effective recognition (requiring technical means to support cross border usage). Thus, the current state of play results from an infraction to the eIDAS Regulation.

> Proposal
>
> To foster the development of interoperability and usage of cross border authentication, article 6 shall be interpreted as relating to an **effective** mutual recognition.

Furthermore article 9(3) states that the Commission shall publish the list of notified eID schemes. However, in the light of the current state of play highlighted above, this information is not sufficient to assess the interoperability of eID schemes, and the possibility of cross border authentication. Therefore, the list defined by article 9(2) shall also indicate the status of effective recognition of eID schemes between Member State (issuing Member State & accepting Member State).

Proposal

The list defined by article 9(2) shall also indicate the status of effective recognition of eID schemes between Member State (issuing Member State & accepting Member State).

Pentesting biometric technologies

Nowadays, there are numerous digital identity systems based on biometric technologies, notably facial recognition. Digital identity systems use facial recognition for enrolment, activation of authentication feature, and service management. In addition, facial recognition is also used by trust services for enrolment.

This widespread deployment of biometric technologies for eIDAS uses, combined with the sensitive nature of biometric data -enshrined in GDPR, makes it all the more important to ensure a high level of security for biometric technologies. This is particularly the case when biometric technologies are used in critical infrastructure (pursuant to the NIS Directive), where resilience against cyber-attacks is key. Therefore, it is necessary to set up requirements on a minimum protection level for biometric technologies, including a requirement to perform penetration testing.

Proposal

Eurosmart recommends performing mandatory penetration testing to assess biometric technologies, as required by ISO IEC 30107 standards on presentation attack detection.

Supplementing attributes for natural and legal persons

Implementing Regulation 2015/1501 (Annex) defines the mandatory and optional data sets for natural and legal persons. This list of attributes is limited to very few elements, hence considerably narrowing a potential cross-border use of eIDs. Many services, such as bank onboarding and healthcare, require additional attributes.

In addition, Implementing Regulation 2015/1501 is also too restrictive in the context of the decentralised provision of identity attributes. eIDAS covers the provision of identity attributes by a sole identity provider, whereas the advent of disruptive technologies sets up a new distributed framework and architecture for the issuance and provision of certified identity attributes. Such identity attributes are delivered by several attribute providers, which is not in line with the current version of eIDAS and its implementing acts. The multi-issuer based ecosystem requires an enhanced definition of personal attributes to allow the provision of attributes by different parties.

Moreover, the eIDAS Regulation requires explicit attributes i.e. all attributes need to be unveiled when proving a digital identity. This approach may be perceived as questioning user's privacy. By contrast, blockchain technology for instance can bring privacy features, by allowing the issuance and verification of personal attributes without unveiling the attributes at stake : a user could prove that he is above 18 without revealing his age. Unfortunately, eIDAS does not encompass privacy preserving uses cases where (1) only a subset of identity attributes, or (2) credentials testifying the user meets a particular set of criteria (majority, location,…) are provided. The variety of verifiable credentials, identity tokens and other certified assertions that are handled by decentralised identity documents on a blockchain should also be taken into consideration, as well as the provision of a subset of identity attributes.

It is worth noting that the recently created CEN/CENELEC Technical Committee on Blockchain and DLT is about to provide Technical Specification on eID requirements pursuant to eIDAS. This Technical

Committee pays special attention to interoperability and regulatory issues, notably compliance of blockchain implementations with EU legislations (such as GDPR, eIDAS, NIS...).

Proposal

-Implementing Regulation 2015/1001 should be reviewed to enlarge the data set defining natural and legal persons with supplemental optional attributes. As such it would be helpful to support sectorial usages that require other data. For instance, it may be useful to consider adding the following attributes:

-Social security number (for healthcare for natural person);

-Medical assurance number (for healthcare for natural person);

-Politically Exposed Person status (for fight against money laundering purposes for natural person).

-Amending current legislation seems necessary to encompass uses cases where user identity attributes are provided by a distributed framework of attributes providers.

-Amending current legislation seems necessary to include privacy preserving use cases that could rely on electronic attestation and blockchain technology.

The need for clearer criteria on assurance levels

The Level of Assurance (LoA) - as introduced by the eIDAS regulation in article 8 - was designed to allow the mapping of trust, and foster cross border authentication between Member States using different criteria, technical and organisational requirements to set up their eID schemes. Implementing Regulation 2015/1502 sets the technical specifications and procedures relating to each LoA (Low, Substantial, High). As such, this concept of LoA was successful in fostering the emergence and deployment of eID in Europe.

However, we observe that there is still no convergence of these criteria, technical and organisational requirements amongst Member States for a given LoA. This is mostly due to the fact that criteria laid down in Implementing Regulation 2015/1502 are too vague and leave too much space for interpretation. A first attempt to refine them was achieved by the cooperation group through a guidance. Nevertheless, these criteria still remain vague, while this document does not have any legal effect, as it is only indicative.

The lack of clarity of these criteria (1) impedes the interoperability of eID schemes and above all (2) prevents Member States from sharing a common understanding of their meaning, which is instrumental for the convergence of practices and eID schemes among Member States.

Today, two eID schemes notified by two different Member States at the same LoA will have to meet disparate requirements imposed by the notifying Member State, as a prerequisite to notification. As such, it creates national barriers causing a market fragmentation.

Proposal

In order to solve these issues we recommend to (1) define clear criteria, which do not leave space to any interpretation, in (2) a legally opposable document (i.e an implementation act and not a guidance).

Furthermore, in order to engage with the industry, it may be useful to task the CEN to prepare a technical standard supporting this implementation act.

In particular, the following aspects should be clarified and refined:

- **Security requirements applicable to "electronic identification mean"** : In order to meet a high level of trust for an eID scheme, a security certification at level "High" -as per EC regulation 2019/881 (Cybersecurity Act)- for LoA "Substantial" and "High" shall be required. This appears necessary as eID scheme is the cornerstone to interact in the digital world and thus access the digital single market. As such, eID scheme is essential to the digital single market, and shall fall under the provisions of operator of essential services (OES) as per NIS directive, justifying to apply such security certification level ("High") benefiting from European wide recognition;

- **The usage of qualified certificate is currently not required** in the Implementation act nor in the guidance, while it is a good practice recognized by the industry. For eID scheme of LoA "Substantial" and "High" relying on PKI based authentication mechanisms, the usage of qualified certificate as defined through [ETSI 319 411-2] shall be required;

- **Validity period of the eID means.** The implementation act and the guidance do not state any requirements with respect to the maximum validity period for the eID mean. However, some Member States define a maximum validity period for eID means of LoA "Substantial" and "High" (5 years), while others do not. As this aspect has direct impact on the level of trust one could confer on a digital identity scheme (why should I trust the electronic identity mean of A that does not have any validity period while B considers its identity mean can not be valid more than 5 years?) , a common approach shall be agreed on.

Improving the management of security breaches

Pursuant to Article 10, only the Member State that has notified an eID scheme is entitled to suspend the cross border authentication means. However, this article does not allow a Member State using and accepting this notified eID scheme -for accessing its public services- to suspend its usage, should it has reasonable doubts or proofs that it contains a security breach.

Proposal
A safeguard clause –allowing a Member State to suspend recognition of notified eID scheme- should be introduced.

Part II: Trust services

Towards harmonised technical requirements for qualified trust services

The eIDAS regulation introduces five types of qualified trust services:

- Qualified validation service for qualified electronic signature (article 33(1));
- Qualified preservation service for qualified electronic signature (article 34(1));
- Qualified validation and preservation for qualified electronic seal (article 40);
- Qualified electronic registered delivery services (article 44(1)).

For each of these qualified trust services, the corresponding article contains the provision defining the requirements to be met. Furthermore, eIDAS introduces provisions empowering the Commission to reference technical standards whose compliance ensures the presumption of conformity to the requirements laid down by the said article. Such provisions were never used. There are international standards such as those in CEN and ETSI, but these are not mandatory today.

Therefore, the technical requirements to be met demonstrating the conformity with the provisions of the article were left to national authorities, leading to fragmentation of the market. More details can be found here.

> Proposal
>
> A harmonised set of technical criteria ensuring conformity presumption to each of these articles shall be defined to avoid market fragmentation.

Harmonising the accreditation process of Conformity Assessment Bodies

The eIDAS Regulation introduces a legal framework and establishes a scheme for granting qualified status to trust services providers. However, there is currently no harmonised accreditation process for Conformity Assessment Bodies (CABs). Eurosmart enjoins the European Commission to adopt a clear and formal harmonisation conformity assessment scheme against which the Conformity Assessment Bodies would be accredited by a National Accredidation Body.

This scheme should be based on ETSI EN 319 403, and promoted at international level. This scheme would give more clarity on how qualified trust service providers (QTSP) are assessed. ENISA[1] pointed out the need to start this process by involving EA, ETSI, EC, ENISA, ESOs. Eurosmart shares ENISA's mindset and recommends as follows:

> Proposal:
>
> -To set up a centralised list of all CABs indicating 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 ».

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

An EU Qualified website authentication certificate

Amongst the electronic services provided by Trust Services Providers (TSPs), website authentication is expected to become a mechanism extensively used. The need for an EU Qualified website authentication certificate (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.

Proposal:

-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 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.

Supporting a Protection Profile for QSCD in the cloud

Eurosmart supports the option of a delegated act for a Protection Profile for Qualified Signature Creation Devices (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 TSPs manage 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 with the QSCD certification. When the QSCD is managed on behalf of the signer, the certification can not be limited to 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, hence leading to market fragmentation. Harmonisation is needed for the electronic signature.

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

Server signing is a valuable achievement to deploy QSCD, it enables a new business model. In to this new approach, the cost of the certificate ischarged 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.

Proposal:
To adopt a delegated act for a Protection Profile for Qualified Signature Creation Devices (QSCD) in the cloud.

Conclusions

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

- Standardisation and harmonisation: creation of a conformity assessment scheme based on ETSI EN 319 403.
- Organisation: enabling a peer-review system for CABs, ENISA can be the peer-review organisation.
- Influence: enhancing eIDAS solutions towards W3C through ESOs and the European Commission. In addition, requesting web browser providers to integrate QWAC.
- Diplomatic: 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 elements, semiconductors, smart cards, secure software, High Security Hardware and terminals; biometric technology providers; system integrators; application developers and issuers.

EUROSMART members are **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, Trusted Objects**, **WISekey**, **Winbond, Xilinx**, **JTSEC**, **Keolabs**, **Serma**, **Brightsight**, **Red Alert Labs**, **Cabinet Louis Reynaud, Trust CB,Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique ToulonSCS Innovation cluster**, **Smart Payment Association**, **SPAC**.

EUROSMART and its members are also active in many other security initiatives and umbrella organisations at 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 contact@eurosmart.com