Comments on eIDAS regulation (EC regulation 910/2014)

September 1st, 2020

ACN's position on eIDAS regulation review

Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organizations (world leaders, SMEs and mid-sized enterprises) operating in France in the digital and electronic trust sector, and especially in the digital identity area.

ACN recognizes the great achievements of the eIDAS regulation but agrees with the fact that the potential of electronic identification and authentification remains underexploited. The eIDAS regulation provides a solid framework from which it is now important to build real interoperability, which is necessary for the development of the digital single market.

ACN is therefore very much in favor of revising this text, which should:

- **Leverage the achievements of the eIDAS regulation, in order for both private and public sectors to effectively benefit from it. The legal identities should become the root of trust of any digital identity issued within Europe.**
- **Enable better interoperability between the different identification schemes from Member States.**
- **Promote the development of an ecosystem of European companies in this field.**
- **Take into account the imperatives of security, personal data protection, protection of civil liberties, as well as European strategic autonomy.**
- **Integrate the European legislative edifice of the Digital Single Market, in particular by relying on the European Cybersecurity Act and the GDPR.**

Therefore, ACN supports option 1 presented in the impact assessment. Suggestions for improvements to this regulation are proposed below.

Nevertheless option 1 could be usefully enhanced by some provisions exposed in option 2. We believe that an effective implementation by the private sector will create adequate level of use for positive experience by European citizens and consumers. It would help structure adequate risk and policy management, and address legal liability regime and compliance. The extension of the scope of the regulation to private actors shall also put in place legal incentives encouraging private sector to issue and effectively use digital identity compliant with the eIDAS framework.

However, full attention should be paid to preserve European digital sovereignty and avoid significant risks on the security of data, particularly with regard to their potential unsolicited use, but also in terms of dependence on major digital platforms. In that respect, storage and processing of personal data related to digital identity shall only be allowed on European soil and with a strict respect of the GDPR provisions.

Concerning option 3, we believe that a successful implementation based on option 1 enhanced by some elements of option 2 will fulfill the expected goal, without introducing a new European digital identity scheme, the articulation of which with all existing initiatives being, in principle, complex. This would lead to render the whole framework unreadable for users, and would therefore slow down the development and use of the multiple existing electronic identity schemes.

ACN's proposals on eIDAS regulation review

Strengthen trust and interoperability in notified electronic identity schemes

Article 7 defines the conditions for notification of an electronic identity scheme. In order to ensure (1) interoperability of electronic identity and (2) trust between Member States, it is paramount that the Member States proposing an electronic identity scheme for notification, as well as all other Member States share the same analysis with respect to the conformity of the proposed electronic identity scheme with the point (a) to (f) of article 7. It would be detrimental for the global trust - and thus interoperability and ultimately widespread use of electronic identity - if an electronic identity scheme were to be notified by a Member State while other Member State(s) disagree(s) with its conformity with the requirements laid down in article 7.

Proposal

To ensure a common agreement of all Member States on the trust of an electronic identity scheme, we propose that:
-the conformity of a proposed electronic identity scheme with each of the criteria defined in article 7 be confirmed by the cooperation group;
-This confirmation be required prior to any notification of an electronic identity scheme.

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 on interoperability framework

This implementation act should be reviewed to enlarge the data set defining natural and legal person with supplemental optional attributes. As such it would be helpful to support other sectorial usages that require other data.

Proposal

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).

COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 on LoA

The criteria defined in this implementation act 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. However 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 electronic identity 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 electronic identity schemes among Member States.

> Proposal
>
> In order to solve these issues we recommend to (1) define clear criteria, which don't 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 of electronic identity scheme, a security certification at level "High" as per EC regulation 2019/881 (cyberact) for LoA "Substantial" and "High" shall be required. This appears as necessary as electronic identity scheme is the cornerstone to interact in the digital world and thus access the digital single market. As such, electronic identity 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 recommended** in the Implementation act nor in the guidance, while it is a good practice recognized by the industry. For certificates derived from an electronic identity scheme of LoA "Substantial" and "High" relying on PKI based authentication mechanisms, the usage of qualified certificate should be required ;
- **Validity period of the electronic identity mean.** The implementation act and the guidance do not state any requirements with respect to the maximum validity period for the electronic identity mean. However some Member States define a maximum validity period for electronic identity mean of LoA "Substantial" and "High" (5 years), while some others don't. 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 doesn't 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;

Management of security breach (article 10)

As per this article, only the Member State that has notified an electronic identity scheme is entitled to suspend the cross border authentication mean. However, this article doesn't allow a Member State using and accepting this notified electronic identity 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 electronic identity scheme - should be introduced.

Effective recognition of electronic identity scheme

Currently the state of play of electronic identity in Europe shows that the notification of an electronic identity 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 electronic identity scheme of LoA "Substantial" or "High" matching the required LoA for accessing the public services "no more than 12 months after the commission publishes the list referred to in point (a) of the first subparagraph".

According to us there are no legal ground for this interpretation sorting out theoretical recognition (notification of electronic identity scheme) and effective recognition (requiring technical means to support cross border usage), and the current state of play results from infraction to eIDAS regulation.

Proposal

To foster 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 electronic identity schemes. However, in the light of the current state of play highlighted above, this information is not sufficient to assess the interoperability of electronic identity 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 electronic identity 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 electronic identity schemes between Member State (issuing Member State & accepting Member State).

Fragmentation of technical requirements for electronic identity schemes

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 organizational requirements to set up their electronic identity schemes. As such, this concept was successful in fostering the emergence and deployment of electronic identity in Europe.

However, we observe that this hasn't yet led to a convergence of these criteria, technical and organizational requirements amongst Member States for a given level of LoA. In other words, two electronic identity schemes

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

Proposal
These criteria, technical and organizational requirements mandated by Member States shall be aligned with the one defined for the LOA in COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502.

Fragmentation of the technical requirements for qualified trust services (article 33(1), article 34(1), article 40, article 44(1))

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, provisions empowering the Commission to reference technical standards whose compliance ensures the presumption of conformity to the requirements laid down by the said article were introduced, but not exercised.

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 at https://ec.europa.eu/futurium/en/system/files/ged/eidas_european_comparison_chart_2017-04-25_0.pdf

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

About ACN:

Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organisations (world leaders, SMEs and mid-sized enterprises) operating in the digital trust sector, such as cybersecurity, digital identity, secured communications, traceability / anti-counterfeiting and safe city. France boasts highly efficient industrial cooperation and internationally recognised excellence in this sector, thanks to world leaders, SMEs, mid-sized enterprises, and other dynamic actors. Currently about 850 organisations in France generate a profit of almost 9 billion euros in this rapidly growing sector (growth of more than 12% every year since 2014). ACN is a founding member of ECSO (European CyberSecurity Organisation). ACN is also a member of the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC - Federation of Electric, Electronic and Communications Industries) and therefore actively participates in the work of the CoFIS committee (Comité de filière des Industries de Sécurité).