Industry views on solutions for eID in Europe

8 July 2022
11:30–13:00 CET

DG CNECT Building
Brussels, Belgium
Presentation on eIDAS 2.0

Maya Madrid
Policy Officer at CNECT.H.4
European Commission
INATBA Policy Position on eIDAS 2.0

Kai Wagner
Identity Working Group Co-chair
INATBA

Establishing a Framework for a European Digital Identity (eIDAS)
Policy Position, July 2022

The International Association for Trusted Blockchain Applications (INATBA) welcomes the European Commission’s proposal for eIDAS, establishing a framework for a European Digital Identity. Our members are supportive of and seek to enable the European Commission’s work to support a transition towards a more digital Europe. The proposal is a key building block towards achieving this objective.

EXECUTIVE SUMMARY

Overall, INATBA supports that:
- the relying party should securely and selectively request only the minimum identity information required to verify an individual’s identity in order to perform a requested service and to determine the authenticity, integrity, and revocation status of the identity information;
- the relying party should not retain, share, or link identity information beyond the extent necessary, and disclosed, to provide the requested service;
- individuals should have the power to securely and selectively disclose the minimum amount of trusted, verifiable identity information required by a service provider to receive the requested service.

INATBA’s position is that the co-legislators should:
1. Support ITRE Amendment #94 which removes the requirement for a persistent, unique identifier that is included in the current proposed Article 11
2. Introduce verifier safeguards into Article 6b to protect EUDISW users from fraudulent requests by relying parties.
3. Retain the proposed Article 6a(l) to allow for competition in the wallet market that will increase user experience and adoption rates.
4. Amend the proposed Article 45E to enable adoption for attestation providers.
5.Extend ITRE Amendment 70 by concretizing the requirement for lifecycle management of the EUDISW that enables control over the EUDISW over time.
6. Amend the proposal, by setting the task to clarify the relationship of eIDAS to public permissionless DLT and blockchain networks in a delegated act.
7. Provide clarity on biometrics-based user authentication for Member States who opt for Proof of Inference in their multi-factor authentication scheme.
Key innovations in eIDAS 2.0

- The **European Digital Identity Wallet** as the common foundation for improved user experience and interoperability
- The **privacy first approach** that aims to protect citizens freedoms online with digital sovereignty
- The introduction of **Qualified Electronic Attribute Attestations** and Electronic Attribute Attestations as a new means of digital credential in line with the conceptual ideas of self-sovereign identity
- The inclusion of **private sector scenarios** and general applicability of eIDAS trust services and ID's beyond the public sector
- The perspective to make **eIDAS based privacy preserving identification and authentication** mandatory as an option at **gatekeeper services**
INATBA Policy positions on eIDAS 2.0

#1: Support amendment 94 to amend the proposed Article 11, by removing the requirement for a persistent, unique identifier as a requirement for the minimum set of person identification data.

Substantiation summary: A unique identifier is not needed for enhanced data subject due diligence and should not be added to the minimum set of person identification data. The risk of misuse outweighs the benefits.
INATBA Policy positions on eIDAS 2.0

#2: Introduce **verifier safeguards** into Article 6b to protect EUDIW users from fraudulent requests by relying parties.

**Substantiation summary:** Relying parties must qualify for requests of PID, EAA, and QEAA data via proof of eligibility to request the data based on clear identification of the purpose and intent behind the request.
INATBA Policy positions on eIDAS 2.0

#3: Retain the proposed Article 6a(1), which authorises Member States to allow for Digital Identity Wallets issued by the private sector.

Substantiation summary: The ability of private sector companies to issue certified Digital Identity Wallets should remain a fundamental principle in eIDAS to enable competition and improve adoption with more choice.
INATBA Policy positions on eIDAS 2.0

#4: Amend the proposed Article 45f, by removing the inclusion of qualified service providers issuing attestations while being the authentic source of the data from the list of providers.

Substantiation summary: Qualified service providers who issue attestations, and are also the authentic source of the data, should be excluded, as they are already covered by article 45a(2).
INATBA Policy positions on eIDAS 2.0

#5: Amend the proposal by introducing a requirement for lifecycle management of the EUDIW that enables citizens to maintain control over their EUDIW over time.

Substantiation summary: The EUDIW providers need to allow for secure and user-friendly approaches to back-up and restore the wallet, as well as the transition of an EUDIW from one device to another when they move to a new phone.
INATBA Policy positions on eIDAS 2.0

#6: Amend the proposal, by adding an empowerment to the European Commission to adopt delegated acts to **further specify how permissionless public blockchains can be used within the eIDAS infrastructure.**

**Substantiation summary:** The European Commission should be empowered to adopt delegated acts which would set out how public permissionless blockchains can be evaluated within the context of the eIDAS infrastructure – potentially under an intermediate level of assurance recognised by potential DLT Trusted Lists.
INATBA Policy positions on eIDAS 2.0

#7: **Proof of Inherence based User Authentication** requires further clarification

**Substantiation summary:** The European Commission should provide clarity on Proof of Inherence based, or biometrics-based, user authentication.
INATBA supports the idea of a unified toolbox for the European Digital Identity Wallet and its ecosystem. Based on our expertise, we recommend to consider the concept of **Self-sovereign Identity** based on the W3C Verifiable Credential Data Model for this common toolbox.

- **SSI is superior** to alternatives in giving users as much **control and ownership** over their **digital identity** information as possible.
- **SSI ensures privacy by design**: the issuer of a particular attribute does not have visibility of where this identity attribute is subsequently used.
- The SSI approach is **consent-based**. This is important for this control and interaction such that only necessary credentials – and additional information – are shared with the third party requesting the ID attribute.
- It **allows for credentials to be shared widely**, without creating one centralised database, or multiple copies of a users’ attributes.
- It is **flexible** since a SSI model can be implemented using either centralised technology, DLTs or a **hybrid setup**.
Other identity working group publications

**Mobile Driver’s Licence (mDL) and Self-Sovereign Identity (SSI) Comparison**

by INATBA Identity Working Group

International Association for Trusted Blockchain Applications

Panel Discussion on eIDAS 2.0

Panelists:

Ms. Maya Madrid – (European Commission) – Policy Officer H4 eGovernment and Trust Unit
Mr. Daniel Bachenheimer (Accenture) – speaking as identity-wg co-chair at INATBA
Mr. Kai Wagner (Jolocom) – speaking as identity-wg- co-chair and board member at INATBA
Ms. Paola Heudebert (Archipels) – speaking as privacy-wg co-chair

Moderator:

Christian Hauschildt (White Research)
Contact
Kai Wagner & Dan Bachenheimer
identity-wg-cochair@inatba.org

Tweet about it:
@INATBA_org
#INATBA