REVISION OF THE EIDAS REGULATION – EUROPEAN DIGITAL IDENTITY (EUID)

INCEPTION IMPACT ASSESSMENT DOCUMENT – ARES (2020)3899583-23/07/2020

September 2, 2020

The undersigned were members of the eID/KYC Expert Group convened in 2018/2020 by the EU Commission which produced two reports released in February 2020 – see links here and here – and welcome the overall assessment and approach taken by the EU Commission with respect to the revision of the eIDAS regulation as shown in the Inception Impact Assessment document (the 'Document'). However, we believe that the current trend towards 'national eIDAS implementations', coupled with a lack of common technical standards for digital identity matters, entails substantial fragmentation risks that need addressing as a matter of priority if there is any hope of achieving a single digital market with the EU. The above-mentioned reports illustrate those risks for the financial sector, with national KYC and identity-proofing rules acting as powerful brakes on the deployment of pan-European solutions.

We strongly believe that eIDAS, in spite of clear limitations, is a landmark regulation that has positioned the EU at the forefront of digital regulatory initiatives since its adoption in 2014. However, digital interactions of EU citizens have considerably evolved since, in particular with mobile device interactions and remote onboarding now the norm rather than the exception, and decentralised technology solutions emerging, bringing a risk of rapid 'regulatory obsolescence' if the current eIDAS regulation is left untouched. We therefore recommend that it be upgraded as well as recognise the mobile centricity of digital interactions as well as the considerable potential of private sector interactions in relation to identity and status attesting, two areas broadly ignored by the current regulatory framework.

This is all the more needed in view of the fact that eIDAS has significantly underperformed delivery expectations regarding the cross-border use of notified digital identity schemes, a situation that in our view has to do with the public-sector focus and inter-governmental perspective of the eIDAS framework for identity-related matters as well as the use of dated technical IT standards for the network architecture (SAML). We view this situation as requiring corrective action if the eIDAS regulation is to successfully address the digital challenge of the 2020s and the digital single market is to become a reality.

In this context, we welcome the three options outlined in the Document and believe that they indeed correspond to the main improvement scenarios, and also concur with the view that they should not be mutually exclusive.

Option 1

Although we clearly consider it useful and indeed necessary, we view Option 1 as best implemented *with* Options 2 and/or 3. Indeed, Implementing Option 1 in isolation – i.e. leaving the eIDAS regulation unchanged - would in our view be insufficient in that it would fail to meaningfully address private sector interactions that we view as key for the implementation of the single market in the digital sphere.

There is however significant room for improvement with Option 1, especially by making wider use of certifiable standards for the purpose of achieving a higher degree of implementation harmonisation – or promoting standards where these do not exist - and adopting further guidelines (instead of non-binding guidances) on specific provisions of the eIDAS regulation.

Option 2

We view Option 2 extremely favourably and believe that introducing new trust services for identification and the provision of attributes, credentials and attestation would be a hugely positive, indeed transformational step, for two key reasons:

- It would plug a huge and critical gap by recognising 'trusted attestations' linking identity and status attributes of EU citizens, whether acting in a personal capacity or in a professional context, including as representatives of legal entities. There are countless use cases where these are needed and could be tailored to meet specific needs – for example, the address, diplomas or professional status of a person could be attested or the KYC attributes of a person could be confirmed (PEP status, good standing, etc.) or a person could simply be attested as being over 18 years old without giving any further details;
- It would meaningfully involve the private and financial sector in relation to electronic attestation services and facilitate the emergence of KYC utilities and dedicated e-attestation providers, therefore fostering a digital eIDAS ecosystem offering usage diversity and scalability.

The Appendix offers a preliminary proposal for Option 2 which we believe is consistent with the current Trust services framework and could be considered to such effect.

Option 3

We have no clear view on Option 3, but this may be due to a lack of information on the nature and scope of the contemplated EUid. We wonder if, as currently contemplated, it would really address the existing eIDAS limitations, especially if adoption is to remain voluntary. We would certainly welcome more information on its practical implementation and in particular wish to understand if would be related to emerging SSI/Self-Sovereign Identity initiatives such as the one prioritized under the European Blockchain Service Infrastructure project.

Stéphane MOUY

SGM Consulting Services
Member of ETSI STF 588

George DIMITROV

Evrotrust

APPENDIX

ELECTRONIC IDENTIFICATION TRUST SERVICES

A new category of eIDAS trust services is to be introduced for the purpose of attesting the identity and/or status of a given person in a given situation or context – the **Electronic Identification Service;**

· **The Electronic Identification Service relates a natural or legal person to a number of identity or status attributes attested by the Trust Service Provider at the time of issuance**. The attestation may cover attribute metadata such as authoritative source, expiry date and level of assurance, which may take the form of an 'AML-KYC grade' (i.e. attribute deemed sufficiently reliable to meet applicable AML-KYC requirements).

· The Electronic Identification Service can be basic or qualified.

  o An Electronic Identification Service is not denied legal effect and admissibility as evidence in legal proceedings.

  o A Qualified Electronic Identification Service is based on a Qualified Electronic Identification Certificate issued by a Qualified Trust Service Provider and containing the relevant attributes and metadata relating to the attested situation;

· A new eIDAS Annex is to detail the requirements for Qualified Electronic Identification Certificates. In order to avoid fragmentation in technical implementation, the Commission is, by means of implementing acts, to establish or refer to reference technical standards for Qualified Electronic Identification Certificates. These standards are to facilitate interoperability and make use of open specifications to the fullest extent possible;

· Attributes and metadata attested pursuant to a Qualified Electronic Identification Service are deemed satisfactorily verified at the time of attestation according to the level of assurance stated for the attributes and/or metadata (for example, the 'address' attribute for 'AML-KYC grade');

· No additional requirements for Qualified Electronic Identification Services is to be introduced by member States – Articles 29, 30, 31 are to apply mutatis mutandis to the requirements for Qualified Electronic Identification devices, the certification of those devices and the publication of lists of such devices;

· Articles 32, 33 and 34 eIDAS are to apply mutatis mutandis to the validation and preservation of qualified Electronic Identification Certificates;

· All other requirements for the QTSPs, such as liability, audits, supervision, etc., continue to apply.