Feedback on the revision of the eIDAS Regulation–European Digital Identity(EUid)

(Inception impact assessment - Ares(2020)3899583)

26 AUGUST **2020**

Association for promotion of digital verification
Skrevet av: Ronny Khan

Introduction

The following team of independent domain experts formed a team “Association for promotion of digital verification” to provide a feedback on the revision of the eIDAS Regulation–European Digital Identity(EUid)

Ronny Khan (https://www.linkedin.com/in/ronny-khan-1b564377/)
Eric Wagner (https://www.linkedin.com/in/eric-wagner-b0a36115/)
Stephane Mouy (https://www.linkedin.com/in/stephanemouy/)
Audrius Ramoska (https://www.linkedin.com/in/audriusramoska/)

General

We concur with the assessments on the description of the current situation. Especially interoperability and extensions to digital validation is crucial if Europe is to have a sovereign common market in 10 years based on the pace of digitalization. There is a clear trend of entrenchment of national walled garden development in this area currently.

As digitalization is happening at different pace in EU we find several member States already implementing digital validation on top of identification. As this happens within the national boundary, we are facing the development of digital islands further weakening the fundament for a single digital market unless common solutions are developed. In our view this is urgent as the resistance will increase dramatically once these islands are entrenched.

We understand that the outlined options are not mutually exclusive and should in all likelihood be combined in order to achieve a satisfactory outcome - for example implementing option 3 appears difficult without inclusion of parts of options 1 and 2.

Option 1

We welcome the suggestion of making specific guidelines on identification which we assume to include fully remote processes and to reduce the emphasis on technology neutrality in favor of being specific to ensure uniformity and alignment in implementations, especially if such uniformity is based on open and already recognized international standards and specifications..

However, we foresee a limited impact of this option compared to the current situation and we view this as baseline requirements which needs to be put in place as a foundation for even considering the next options.

Option 2

We fully support the notion of provision of attributes and attestation of those. In terms of organization we are doubtful if this should be organized as trust services per se. In our view the source holding the information needs to be qualified and provide easy to check seals to the attestation, but we do not see this as a trust service in the normal definition of this terminology. In terms of financial services an entity holding a banking license should be able to emit attested KYC data without becoming a trust service provider or regulated other entities like a Notaries, companies that provide various registries services or local municipality authorities. Such approach will allow market participants to compete in related service delivery, each market participant could decide which level of trust is enough for him. We believe this is the case for most use cases including attested attributes and where a requirement

defining this as a trust service will only introduce a middleman providing little value and obscuring the source and the responsibility of the attributes.
Trust service providers could coexist in such market, their services could be mandatory in some use cases.

To capture the value of this suggestion the required attributes need to be defined and harmonized between the member states, including the additional regulatory required attributes especially for the Financial Services sector. We also recommend that market participants should not be prohibited from further additional non-regulatory required attribute provisions that could be related to the particular industry or a region as example. However care must be taken since there is an inherent risk to create a non harmonized market by inclusion of such «local» attributes.
If these recommendations are not implemented, question remains if Option 2 provides value at all for cross border usage and for enhancing a single digital market. For the financial market this was indeed the conclusion of the EU expert group.

Furthermore, we recommend

- an extension of minimum mandatory identification attributes to a full set of identification attributes, ideally complemented with due diligence attributes so that a KYC process could be fully digitized
- a shift from central gateways (such as fully centralized eIDAS nodes and federated eID approaches) towards decentral nodes acting as trusted source gateways for respective KYC attributes, enhancing data protection/data privacy (a single node should not know every customer interaction) and increase cyber security (node redundancy)

We cannot see option 2 being put in place without 1 being done as a precursor. In our judgement this option will have a significant beneficiary impact if data standardization pertinent to use cases is done also. If no such data sets are defined the benefit could be questionable.

Option 3

We believe a common scheme would provide an invaluable strengthening of the use and deployment of electronic identity. A fully harmonized eID scheme covering Europe would move from the current widely different schemes toward one common standard which would significantly contribute towards adoption both from a purely technical and economic perspective, but also increase the adoption in terms of ease of acceptance and usage. However, we believe this should be sought in a public private cooperation.
This option would enable a market competition to take effect and where we would hope to see a pattern similar to what has been seen in the payment industry.

The authoritative source for onboarding an identity would be a member state.
The entities onboarding would be highly regulated and/or supervised public and private entities.
The form factor of the identity would be highly standardized to ensure portability in the same way passports have always been and identity cards are becoming based on the EU wide standardization of national ID cards mandating adherence to the ICAO standards.
Acceptance would at least follow the patterns we see from passports and payment cards where offline validation will be predominant and optional online verification can be accomplished subsequently at the issuer. Ideally verifications are done online in realtime with offline capabilities (f.ex. via mobile phones or NFC cards or similar)

We see the merits of enforcing acceptance and mandatory notification of national schemes but question if such measures will not be seen as to prescriptive and would raise questions about big brother and privacy and remove the focus from the inherent value propositions offered.

Again, we see very little rationale for option 3 unless option 2 and 1 is implemented as precursors.

In terms of impact we do not see a major contribution from Option 3 on itself. The major benefit of Option 3 would be to enhance the uniformity and harmonization in the area thus probably giving a higher adoption even without a prescription on acceptance.
The combination of this increase in adoption and the benefits brought by Option 1 and 2 will only together give a much needed enhancement and push towards digital sovereignty.

Final observations

Conclusions

The current eIDAS regulation update will significantly impact EU and national digital developments, related investments and digital environment role within EU and Member States during upcoming years. Therefore, eIDAS regulation update should incorporate the major aspects from all options and if necessary, updated with the reasonable new options proposed during the current consultations.
In terms of enabling a deep single digital market the addition of attributes and defining cross border data sets is crucial for enabling digital verification at the European level and to avoid the member states turning into digital islands. This is fully inline with the recommendation in the CEPS report but will require a deployment of solutions to happen at scale in the MS where standardisation and harmonisation are key enablers.
This would be instrumental in promoting the same goals as the single digital gateway and the only once principle also for the private sector.

Recommendations

Our recommendation is to implement all three proposed options in a coordinated approach, f.ex. first the harmonized attribute definitions, then the trusted service provider determination, followed by the respective liability framework and lastly by the necessary RTS. Such approach will allow to prepare for the subsequent option components implementation be implemented in a more efficient and effective way, collect as much as possible feedback from the market and MS and could reuse the latest technology developments in that field.