Erste Group Bank Feedback on the European Commission's consultation on a roadmap for the revision of the eIDAS Regulation

In general, the Commission's assessment of the current situation seems adequate, especially since interoperability and extensions to digital validation are crucial for a sovereign digital market in Europe. Because of the different pace of digitalization across the EU, several Member States have already implementing digital validation on top of identification. This leads to fragmentation which further weakens the fundament for a single digital market unless common solutions are developed.

When it comes to the 3 options outlined in the roadmap, we believe that the they should not be mutually exclusive but instead be combined in order to achieve a satisfactory outcome. For specific remarks and recommendations, please see the comments below.

Specific remarks on Option 1

We welcome the suggestion of making specific guidelines on identification which we assume will include fully remote processes and will 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 see a limited impact of this option compared to the current situation and we view this as minimum requirements which need to be put in place as a starting point for even considering the next options.

Specific remarks on Option 2

We fully support the notion of the 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 another regulated entity like 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 a market and 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, 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, for instance. However, there is an inherent risk to create a non-harmonized market by inclusion of such local attributes. If these recommendations are not implemented, the question is whether Option 2 provides value at all for cross-border usage and for achieving a single digital market. For the financial market this was indeed the conclusion of the EU expert group on remote KYC.

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 Option 1 as a precondition. In our view 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.

Specific remarks on 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 in the EU would move from the currently very 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. We believe this should be developed through a public-private-partnership. This would enable market competition to take effect and result in a situation similar to 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 real-time with offline capabilities (e.g. via mobile phones or NFC cards or similar).

We see the merits of enforcing acceptance and mandatory notification of national schemes but would fear that such measures could be seen as too prescriptive and raising questions about privacy and remove the focus from the inherent value of the proposals.

As already mentioned in the context of the other options, we see little rationale for Option 3 unless Option 2 and 1 are implemented, as well. 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 uniformity and harmonization and thus probably lead to a higher adoption even without a prescription on acceptance. The combination of this increase in adoption and the benefits of Option 1 and 2 will together give a much-needed enhancement and push towards digital sovereignty.

Conclusion

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, the eIDAS Regulation update should incorporate the major aspects from all 3 options.

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 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, e.g. 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 that the subsequent option components will be implemented in a more efficient and effective way, allow to collect as much as possible feedback from the market and Member States and the reuse of the latest technology developments.