bitkom

At a glance

eIDAS review & EU digital ID

Starting point

On 3 June 2021 the European Commission presented the proposal for a regulation on the EU digital ID and the review of the eIDAS regulation. The proposal seeks to promote the use of digital identity and among other things comprises introduction of the ID wallet which citizens can use to identify themselves digitally as well as store and manage their identity data and official documents in electronic form.

Bitkom assessment

Goes in the right direction: the proposal to establish the EU ID and wallet is an important step. **Our objectives are** a high level of acceptance, market openness, European harmonisation as well as Europe-wide application possibilities.

Most important finding

The details of the proposal leave some questions open and need to be revisited, in particular with regard to the following points:

- **Technical details, standardisation and interactions with other regulatory provisions**
  Technical details of the design of the wallet and the standards on which it is based have not yet been definitively clarified and need to be developed in joint consultation with industry. In addition, it is absolutely essential to ensure coherence in the regulatory framework.
- **Successful implementation in the market**
  In our view, the EU should strive to enable multiple certified wallets to coexist in the market in order to have successful competition with the best possible solutions and successful implementation of the wallet. The EU should lay down harmonised, realistic and workable certification requirements.
- **Incentives for use without blanket compulsion**
  We are convinced that the EU should encourage the Member States to offer digital solutions which are sufficiently attractive and convincing for users to take them up. A blanket obligation with no differentiation imposes unnecessary efforts, a high degree of uncertainty and costs on companies in the private sector.

Summary

Bitkom welcomes the European Commission's draft since it lays a further important foundation stone for secure identities and trust services in the European Union. Europe's digital sovereignty is strengthened if digital identities are established and can be used autonomously by EU citizens Europe-wide. Bitkom is grateful for the opportunity to set out its position in the framework of the consultation process.

The European Commission has rightly recognised that digital identities should continue to be made available under the sovereignty of the Member States. Similarly, the introduction of new trust services is a useful complement to the network of trust services which stretches across Europe. In addition, Bitkom is pleased that the overall aim is an eID ecosystem with appropriate connectivity to other European initiatives (such as the Digital Markets Act (DMA) and the Digital Services Act (DSA)). In this connection, the obligation to have user-friendly qualified website authentication certificates (QWACs) is particularly positive.

However, in our view, the details of the proposal still need some adjustment in order to achieve across-the-board implementation, user-friendliness and acceptance. We believe that this can be brought about only through transparent and broad-based involvement of industry in development, design, standard-setting and further requirements on the wallet and its use. Coherence across the entire regulatory framework should be ensured by the same token. Furthermore, we are convinced that the EU should encourage the Member States to offer digital solutions which are sufficiently attractive and convincing for users to take them up. A blanket obligation with no differentiation imposes unnecessary efforts, a high degree of uncertainty and costs on companies in the private sector.

The EU should also strive to enable multiple certified wallets to coexist in the market in order to have successful competition with the best possible solutions and successful implementation of the wallet. The EU should lay down harmonised and practical certification requirements.

Detailed assessment

We examine below what we regard to be the most relevant details of the draft regulation.

1) References to natural and legal persons

Bitkom welcomes the proposal that the wallet should also be introduced for legal persons. But it should be clarified in sections I-III which provisions apply for natural and/or legal persons. The same applies for "personal data" and "person identification data".

Moreover, eIDAS 2.0 should also clarify that both the EU digital wallet and national as well as private schemes together with associated provisions apply for legal and natural persons alike insofar as a special stipulation is not necessary for an individual provision.

2) Article 3d): Inclusion of identification services in the list of trust services

In accordance with article 24, "identification services" are a central aspect of trust services and should be regulated as a stand-alone trust service. The possibility should be added that identification services can also be verified and listed as qualified trust services. This would ensure harmonisation of the various levels in an identification procedure and an approximation of the security level. There are currently widely divergent provisions, leading to a distortion of competition.

During verification, appropriate technical standards such as ETSI TS 119 461 should be adduced for classification of the trust level.

Alternatively to regulation as a stand-alone trust service, it should at least be ensured that harmonisation at European level is both based on technical standards and involves harmonisation of the certification requirements of conformity assessment bodies.

3) Article 6a (introduction of a European Digital Identity Wallet)

The EU should strive to enable multiple certified wallets to coexist in the market in order to have successful competition with the best possible solutions and successful implementation of the wallet. The EU should lay down harmonised and practical certification requirements.

Furthermore, it should be clarified in article 6a paragraph 3 b) that signature with qualified electronic seals in the wallet is also possible alongside the qualified electronic signature.

With regard to article 6a paragraph 3 b) ("European Digital Identity Wallets shall enable the user to: [...] (b) sign by means of qualified electronic signatures"), it should be ensured that the wallet serves as an identification and authentication instrument for the use of a qualified electronic certificate issued by a QTSP which has been *freely chosen* by the owner of the wallet (or, depending on process and use case, by the relying party). There is otherwise the danger that this free choice could be "restricted" if the wallet provider is itself active as a QTSP (with negative consequences for fair competition in the digital single market or a facilitation of monopolies or dominant positions).

For the success of the EU wallet, it must be ensured that all verifiable attributes can be shown, for instance proxy powers recorded in registers. An exclusion would unnecessarily restrict the use scenarios and hence the success of the EU wallet.

4) Article 6b) requirements on relying parties

It is intended that legal persons should use the EU digital wallet actively to the widest extent possible. Accordingly, legal persons which register as a relying party should be required to use an EU digital wallet themselves.

However, the requirements regarding procedures applied by relying parties and the verifications to be performed need to be defined in closer detail and concepts need to be clarified.

5) New certification requirements for the wallet (article 6c)

Article 6 of the 2014 eIDAS regulation, which provided for a mutual recognition of eIDs, has been superseded by new provisions on the EU digital identity wallet (article 6 a-d). Just like other electronic means of identification, the wallets must be recognised by the Member States (article 12b and c). At the same time, certification standards which the wallets must meet are specified (article 6c (4)).

We welcome the envisaged implementing acts (article 6c (1)). They will lead to greater harmonisation of requirements. This will make them easier for EU citizens to use and their reach will be enhanced.

6) Article 10a (occurrence of security breaches)

Under the Commission's proposal, the issuance and validity of the digital wallet would be suspended when a security breach occurs.

We believe that clarifications are needed here. The availability of ID wallets is of eminent importance in the areas of both autonomy and business activity. A "resilience" qualification is needed here in order to ensure that further use is still possible (in analogue form if necessary) when the system is compromised**.**

7) Article 11 a (2): legal persons must also be given a unique and persistent identifier

We support the requirements for giving a unique and persistent identifier to natural and legal persons, and call for this identifier to draw inspiration from international specifications, for example in accordance with ETSI. Cf. section 5.1.4 ETSI EN 319 412-1 (2020-07)

With regard to legal persons, a reference to the possibility of using an LEI (Legal Entity Identifier: https://www.gleif.org/de/about-lei/introducing-the-legal-entity-identifier-lei) would be desirable.

8) Article 12b: acceptance of the wallet

The Commission's draft provides that numerous private service providers would automatically be obliged to accept the European identity wallet alongside very large online platforms as defined in the Digital Service Act (see article 12b (2) of the draft). The objective pursued here is obviously the widest possible dissemination of the European digital identity wallet. An obligation on entire sectors with no specific reference to defined relevant use cases for citizens is too broad. The Commission proposes that stakeholders from numerous sectors should be obliged to accept the EU digital identity wallets where they are required by national or EU law or by contractual obligation to use strong user identification for online identification. It is our conviction that the EU institutions should encourage the Member States to offer digital solutions which are sufficiently attractive and convincing for users to take them up. A blanket obligation with no differentiation imposes unnecessary efforts, a high degree of uncertainty and costs on companies in the private sector. Without clear framework conditions as to when a company would be covered by the obligation, adequately long transition periods based on user numbers and a strict delimitation of the regulation to genuinely relevant use cases, an absence of acceptance can be expected on the part of the private sector.

9) Article 24c (harmonised certification of trust services)

The European Commission will adopt markedly more implementing acts which refer to international technical standards, e.g. those adopted by CEN and ETSI. The requirements for certification of trust services can be better harmonised through these implementing instruments. ETSI has already published a new standard ETSI TS 119 461 for article 24c which the Commission should accept.

We welcome the European Commission's effort to harmonise the certification of trust services further. In this connection, the systems authorised hitherto on the basis of "comparable security" might no longer be acceptable in the medium term. It would be sensible and desirable to enact a transition period for such cases**.**

10) Article 45 a-f

a) New trust services

New trust services are expected to complement the trust area stretching across the EU. These include trust services providing electronic archiving and electronic attestation of attributes, management of electronic remote signature and seal affixation devices or electronic ledgers.

In our view, the new trust services offer great opportunities for the digital single market.

b) Specifications needed

This also applies for introduction of the new qualified "electronic attestation of attributes" trust service comprised in the draft, which we welcome in principle. Because the logical extension to the trust service set out in section 9 of the draft regulation (article 45 a-f) is citizen identity data. However, it is not clear from the draft how such a trust service would function across all EU Member States. For reasons which are difficult to understand, many urgently necessary specifications are deferred for inclusion in subsequent implementing acts.

Moreover, the various responsibilities between national states and trust service providers are not worked through in the draft. For example, it is not clear under what circumstances designated intermediaries can act as a source or when a national source must be involved. Hence, it remains unclear who at federal or central level has to create the requested possibilities for electronic access to "public sources" in federal entities. Rather, it is essential to specify exactly how the trustworthiness of sources can be established and maintained in the long term.

The draft also appears difficult to understand with its demand in article 45f (4) whereby a trust service may only be operated under a separate entity. What is the justification for this? How does the "quality" of this trust service differ from others where this requirement does not apply? In our view, it is urgent to differentiate between wallet providers and providers of the various qualified attributes in the wallet. Under this scenario, the requirement as set out would apply only for wallet providers but not for suppliers of attributes. Setting up a separate legal entity would result in an additional hurdle for suppliers of trust services.

A security gain through a legal separation arises only for the supplier and operator of the wallet which as data intermediary has to be excluded from onward use of the data acquired. For greater transparency and security, we think it a good idea to be able to refer to a European trust list on which the sources of qualified attributes are recorded in a uniform manner and which can be drawn on publicly for validation of everyone, along the lines of the *European Trustlist*.

c) QWACs

The proposed visualisation of QWACs is a milestone for the digital single market and strengthens European consumer and data protection. Visualisation of QWACs is an important measure which leads to greater transparency and data protection in the digital world.

11) Article 45 f: additional rules for the provision of electronic attestation of attributes services

Restriction of personal profiling is under intensive discussion at this time but has also already been addressed in law. In any event, the current formulation goes beyond the requirements of GDPR.

We propose that article 45f be scrapped in its entirety and that the requirement be replaced in article 6a 7) by a reference to the applicable provision of GDPR.

12) Backup possibilities

It must be borne in mind that citizens frequently change and sometimes lose their smartphones. This circumstance should be taken into account and the need for an encrypted backup is therefore very important. It is not clear in the draft regulation what a solution might look like.

We believe that an HSM-supported server backup or similar could be useful here. These systems can be implemented in such a way that it is not possible for even the provider to access the data while at the same time the necessary strong customer authentication (two factor) for recovery of the backup is ensured.

13) Toolbox

The expert group which is devising the toolbox should also be complemented with representatives of professional associations and private providers. This know-how and the interests of the latter must also be represented, in particular so that aspects linked to international standards, intellectual property, data and know-how protection can also feed into the discussions. If the objective is an open ecosystem, the expert groups must also be structured accordingly in an open and transparent way.

14) Authentication / biometry

Use of the EU eID wallet will depend essentially on its usability. Use of a PIN on its own has proved not to be secure and is not user-friendly. Biometry as an authentication procedure should be made possible. Along the same lines, thought should be given to a certification program for the security level of biometric sensors.

15) Open ecosystem / freedom of choice

In order to achieve the objective of an open ecosystem, a particular focus should be placed on the interoperability and transferability of identities and attributes in the wallets. For example, to establish a European ecosystem, it should be possible to insert the identity of a German citizen in the wallet of another Member State (e.g. a French EU eID wallet). Similarly, citizens' freedom of choice must be maintained and it must be ensured that the draft regulation opens up the possibility for a citizen to transfer his identity between two certified wallets. This also results from the need to enable a backup: a transfer to a new device must be possible here, as must an encrypted backup.

16) Data protection and cybersecurity (in particular in the context of the NIS-2 directive)

Data protection, digital trust and cybersecurity are the three pillars of the digital world, and Europe points the way for their regulation with GDPR, the eIDAS regulation and the NIS directive(s). The proposal underlines the need for digital wallets, QTSPs and trust services to deliver a very high level of security, and provides

in article 24 a) that QTSPs must comply with article 18 of the NIS-2 directive. Although we concur with the principle, we must point out that this runs the risk of possible future variations between the security risks for QTSPs in different Member States, a situation which is detrimental to harmonisation. Since NIS-2 is a directive, each Member State can support a different interpretation in the transposition phase; if we also consider that the NIS supervisory bodies may differ from the eIDAS supervisory bodies, there is a possibility of conflicts which could have implications for the harmonisation and costs of providing similar trust services in the EU. To circumvent this problem, it is therefore very important to have strict coordination between the Commission, ENISA, the cooperation network and the NIS supervisory bodies as well as clear guidelines for QTSPs as to what requirements they should meet, for the supervisory bodies when conducting the supervision process and for CAB so that approaches are harmonised during audits.

Article 3 point 53 of the eIDAS proposal introduces the definition of the "electronic ledger" ("tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering"). The definition is very open and, even with the help of recitals and other references, it is not clear what the regulation's objective is on this issue, neither is it clear what the "electronic ledger" actually is according to this article. It could be useful to clarify the following points better:

a) According to recital 34 of the preamble, the objective of the regulation is that a qualified electronic ledger should enable a governance framework and SSI. The current eIDAS regulation already pursues a centralised approach with regard to identity, but if the objective of the new proposal consists in moving to a highly decentralised solution, this should be expressed more clearly.

b) Under the definition of "electronic ledger", many instruments could already today ensure that data time stamps cannot be changed – and are also used for this purpose. It could be useful to add more details to provide an understanding of the value offered by a new qualified trust service and to highlight what tasks an "electronic ledger" can perform better than the existing trust services. This clarification will also prevent duplicate regulation on the issue: many electronic ledgers used today by governments and companies are already regulated in the Member States.

17) Active participation of authorities

Taking the lead from the EU proposal, Member States' legislation should routinely oblige authorities in all relevant specialist laws to take part in the various roles in the

ecosystem and also actively deploy existing trust services (e.g. electronic seal and newly established means (electronic means/attestations).