WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021) 281 final)

Berlin, 08.05.2023

With the eIDAS Regulation, the EU created a uniform legal framework for trust services and electronic identification throughout Europe. The aim was to increase the use of trust services for cross-border transactions in the digital space through common standards in the area of online signatures or electronic seals, and to contribute to the digital single market.

Part of the existing regulation, which has been in force since 2016, entails an evaluation of its effectiveness. This was carried out by the European Commission in 2020. The Commission concluded that, in particular, the potential for the use of electronic identification is not yet sufficiently utilised.

As a result of the evaluation, the Commission outlined three options to increase the use and diffusion of electronic identification means. These ranged from minor adjustments in the implementation of the regulation to the final chosen option of revising the regulation and creating a framework for an EU-wide interoperable European Digital Identity Wallet (EDIW). eco spoke out in favour of the option chosen here in the consultation on the Impact Assessment and supports the Commission's approach in principle.

Digital identities are not just an important prerequisite for a digitalised government, but also the foundation for many business models. In this context, action at EU level is important so that the wallets established by this proposal can be used throughout the EU to make use of public or private services, and to thus advance the digital single market and European integration as a whole.

In detail, eco has the following comments on the opinions of the Parliament and the Council, which should be taken into account in the trilogue:

▪ Issuance of the European Digital Identity Wallet

In the report of the European Parliament, the wording concerning the issuance of wallets was changed in some important points. One specific point is that the Member States "shall issue at least one European Digital Identity Wallet".

In the Council's text, the Commission's wording was retained, according to which the states should only ensure that wallets are available to all citizens.

In the Parliament's report, changes were also made to the various ways in which the wallet can be issued, while the Council kept the Commission's

proposal regarding which EDIWs were to be issued either “by a Member State; under a mandate from a Member State; or independently but recognised by a Member State”. The Parliament’s version, on the other hand, states that they “shall be issued and managed in one of the following ways: directly by a Member State; under a mandate from a Member State; or independently from a Member State but recognised by that Member State”.

eco is in favour of an ecosystem that is as open as possible and that allows the development and issuance of EDIW by as many actors as possible. In its draft of the new eIDAS Regulation, the Commission itself states that users are already accustomed to convenient and easy-to-use private sector authentication solutions. This is also due to the mostly high level of user comfort. The proposal of the Commission should therefore define uniform criteria and open standards according to which EDIW can be developed, issued and certified. For this reason, we are in favour of a formulation in the text of the regulation that also provides for the issuing of wallets by private sector actors and allows competition for the best and most user-friendly identification solutions. Government recognition of the EDIW can contribute to trust and acceptance in the wallet ecosystem, but should not be mandatory.

- **Assurance level of the European Digital Identity Wallet**

Article 6a (6) in the report of the Parliament as well as the general approach of the Council states that “the European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance ‘high’”. eco views this decision critically. In many European countries, the only possibility of notification according to the level of assurance is the use of the national eID solution, which is often linked to the national, government-issued identity cards. In our view, the identity card or an identity derived from it should not be a prerequisite for the use of an EDIW. Its use should only be mandatory in specific cases where a high level of assurance is absolutely required, such as for some public or banking services. The wallet must provide various options for users to choose from when it comes to identification and authentication. In this context, it should also be pointed out that, when it comes to some public services, they too do not necessarily require this high level of assurance.

The use of a government-issued eID for all use cases would also not be desirable, especially from the point of view of data protection. A link between a government-issued eID and the EDIW could increase the potential for misuse and profiling. For this reason, a decentralised system using different means for authentication and identification would be favourable in our opinion. For users, the use of an EDIW should also be as simple as possible and not dependent on any prerequisites.

- **Functions of the EDIW**

In their drafts, both the Parliament and the Council include a number of functions for the EDIW that go beyond pure identification and authentication.

It would also be possible to generate electronic signatures or seals with the help of the wallet. The Parliament's report also provides for the possibility of creating pseudonyms to make pseudonymous use possible. In addition, both the Parliament and the Council call for an archiving function that allows users to view and record all access by relying parties to their attestations of attributes. Archiving is intended to prevent unauthorised access to data, attestation of attributes, or credentials. The EDIW should also offer the possibility for end-to-end encrypted exchanges with relying parties and other European digital identity wallets. The Parliament and the Council also call for the encrypted exchange with trusted parties and other European digital identity wallets and envisage the function of being able to use the wallet offline in their positions. For this purpose, it should be possible to store and retrieve the attestations of attributes locally.

eco supports a high level of data protection and data security regarding the EDIW. With the GDPR, Europe has a strong and globally recognised framework for the protection of personal and sensitive data that is already in place. The requirements for the EDIW in the area of data protection should therefore refer to the GDPR, wherever possible. For us, trust in the security of one's own sensitive data, in addition to a user-friendly design and a high number of use cases, are basic prerequisites for a successful implementation of the wallet and the greatest possible acceptance among citizens and businesses.

However, the extent to which all of these services and functions have to be provided by the issuer of the wallet should be examined. eco is of the opinion that, also in the interest of competition, the wallet as a whole should be designed in such a way that the most diverse providers of trust services such as seals or signatures are able to integrate it into their services without any difficulties. To achieve this the wallet would have to provide open interfaces. We support the possibility of offline use in the context of the most comprehensive use possible by the users. We also endorse the requirements for security-by-design and end-to-end encrypted communication with relying parties. User trust is an important factor for the success of the wallets, especially since some of the data concerned is considered to be particularly sensitive and protectable.

- **Approval obligation for relying parties**

In their negotiating mandates, the Parliament and the Council follow the Commission's draft with regard to the obligation of relying parties to register in the Member State in which their registered office is established. In the Parliament's report, this obligation also does include information about the data that the relying party is intending to request for each of its services. While it is understandable that the Parliament wants to prevent the misuse of data and information, it should be noted that these obligations could impose a high bureaucratic burden on the relying parties; especially if, as envisaged by the Parliament, they have to provide detailed information on the data requested for each service.

The extent to which these obligations are really necessary to enable trustworthy use should be examined. For a successful EDIW, it is essential that it can be used for as many use cases as possible. Obstacles for relying parties that offer these use cases could damage the acceptance of the wallet in the market and ultimately lead to users not being able to use their wallet for authentication for many services in the private sector.

- **Acceptance by the private sector**

The new eIDAS Regulation stipulates that the EDIW must not only be accepted by public institutions, but also by some actors in the private sector. The regulation specifies certain sectors in which service providers are obliged to accept the wallet. These include the banking sector, the telecommunications sector and health services. In addition, according to the DSA, very large online platforms (VLOPs) must also accept the wallet as a means of identification and authentication.

eco rejects an obligation for private actors to have to accept the EDIW. We share the Commission's goal of achieving the broadest possible use of the EDIW and recognise the added value of an interoperable identification solution that can be used throughout Europe for many private business models and companies. In order to achieve real acceptance in the market, however, we believe that it is essential for service providers and users to be able to use the system as conveniently as possible. An obligation for different providers to accept a certain product for authentication interferes with the private autonomy and design of the services of the companies and also leads to additional costs. Acceptance among companies for the use of the EDIW should primarily be achieved through open interfaces and a simple integration of the EDIW into the services of various providers. In eco's view, this would be the most successful way to achieve broad acceptance in the market, even beyond the sectors envisaged in the draft.

- **Open source and interoperability**

The Council and the Parliament also made changes to the regulation with regard to the technical design of the EDIW. According to the Parliament's report, the source code for the EDIW should be published as open source, which should make it possible for reviews and verifications, among other factors. In addition, the European Parliament addresses interoperability obligations. According to this, users should be able to switch easily between different wallets at any time. In this context, the draft provides for a right to data portability.

eco supports competition between different providers for the best and most user-friendly EDIW. As such, we generally support measures that allow users to easily switch between different wallets. Nevertheless, the requirements for interoperability should not lead to a situation where competition for the best solutions is no longer possible and a forced alignment of the different wallet solutions occurs. The obligation to disclose the source code of the EDIW is also problematic from the point of view of the Internet industry. EDIW providers should not be obliged to make their source

code accessible to competitors as this could disclose trade secrets. Moreover, it would restrict the design of the EDIW, also with regard to possible additional functions. From our perspective, the focus of the specifications for the design of the wallet should rather be based on open standards.

- **Communication of advantages**

The Parliament's report calls for measures to promote the EDIW on the part of the Commission after its introduction, and to create awareness of the advantages of the EDIW. eco expressly supports the position of the Parliament. The creation of a cross-border ecosystem for digital identities in Europe should not be thwarted by too little awareness of the EDIW and its advantages. Not only the provision of information, but also the tackling of questions or uncertainties in the context of the EDIW should be considered in the process and are necessary to achieve a high level of social acceptance for the new wallets.

- **Regulation for providers of web-browsing services**

In Article 45 (2), the new eIDAS Regulation establishes new regulations for the providers of web-browsing services, obliging web-browsers to recognise Qualified Website Authentication Certificates (QWACs). Web-browsers would also have to display information on QWACs "in a user-friendly manner" on their User Interface (UI). For these purposes, browsers are required to accept these certificates as secure without any quality control on the Certificate Authority (CA) and thus regardless of whether there are malicious behaviours towards browsers' users, such as domain impersonation or phishing. However, experience shows that issuing QWACs does not prevent certain CAs from misbehaving. eco assesses this step as comprehensible but views it somewhat negative. Therefore, Article 45 should be amended to allow web-browsers to react to breaches of security and to take precautionary measures. Web-browsers should participate in a collaborative manner with European Institutions in a procedure of measure validation. Moreover, any UI lay-out obligations should be established after market consultation of all relevant stakeholders in the web-browsers' chain.

- **Conclusion**

eco supports the initiative for a European Digital Identity Wallet in principle. A reliable and secure ecosystem for digital identities is a cornerstone for the realisation of the Digital Single Market and a multitude of business models. In addition, EDIWs that can be used throughout Europe are a prerequisite for cross-border usability and digital public administration with all its benefits for citizens, companies and governments. However, when it comes to the concrete design, we would like to point out the following factors that should be taken into account during the trilogue in order to enable a successful implementation:

- An open ecosystem is necessary
  One of the aspects that the market will depend upon in accepting the wallet is user-friendliness. The provision of the EDIW should therefore be market-based, and competition between different providers for users through user-friendly solutions should be encouraged. The policy should define the standards according to which a wallet can be certified as an EDIW wallet. We, therefore, reject a government monopoly in the development and issuance of the EDIW.

- Enable easy usage
  The use of an EDIW should be as simple as possible. As such, we critically review a required notification according to the “high” trust level. In principle, it should also be possible to use the wallet without prior notification and the use of a government-issued eID. This should only be necessary for specific use cases that require the “high” trust level. Hurdles to the use of the EDIW should be kept as low as possible. Notification through an eID also increases the risk of profiling based on a state-provided identity.

- No mandatory acceptance by the private sector
  We reject a blanket obligation of certain private sectors or so-called “gatekeepers” to accept the EDIW as a means of authentication. In our view, the focus should be on making the EDIW as easy as possible to integrate and use in existing services. An obligation for different providers to accept a certain product for authentication would also infringe upon the private autonomy and the design of the services and would also lead to additional costs for companies.

- Enabling innovation
  Interoperability between different wallets is fundamentally in the spirit of competition for the best solution, as it prevents log-in effects for users and facilitates switching between providers. Nevertheless, interoperability rules must not be too rigid and must continue to allow for innovation and different wallet designs. We are also in favour of open standards. On the other hand, we reject an obligation to publish the source codes of EDIW.

- No barriers for relying parties
  In order to make the use of the wallet as simple as possible for the relying parties, eco recommends keeping the requirements regarding a possible registration obligation as low as possible. Businesses that want to accept EDIW as a means of authentication should be able to do so without too much bureaucracy and costs. With their services, the relying parties offer important use cases that are indispensable for the acceptance of EDIW.

- High requirements for security and data protection
  The EDIW must have a high security standard and a high level of data protection, as provided by the GDPR. Security-by-design and user-centric management of access rights should form the core of the technical design of the wallet. Especially with sensitive personal information, trust in the security and protection of this information is particularly important for many users. In order to effectively prevent profiling, it is also necessary to be able to use different means of authentication side by side for different use cases in order to effectively ensure decentralised data management.

- Provide communication support for the introduction of the EDIW
  The introduction of the wallet should be accompanied by information campaigns. In addition to the advantages and possibilities, questions and uncertainties should also be addressed.

- No new regulations for providers of web-browsing services
  The free product design of browser providers should not be restricted by the new regulations. In our view, the political specification of certain certificates is not appropriate. The decision as to which certificates are recognised and displayed should be made by the browser providers themselves or in collaboration between browser providers and European institutions in the interest of the users.

About eco

With more than 1,000 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust and ethically oriented digitalisation. That is why eco advocates for a free, technology-neutral and high-performance Internet.