

# Revision of the eIDAS Regulation

## Findings on its implementation and application

### SUMMARY

The European Commission's proposal (June 2021) for a European Digital Identity Framework would provide a trusted and secure way to authenticate and share qualified data attributes online through a 'digital wallet' ensured by Member States and allowing transactions across the EU. If put into effect, it would aim to achieve the target set in Europe's 'Path to the Digital Decade', which envisages 80 % of EU citizens using digital ID by 2030. It would also execute the European Council's vision and explicit request for EU-wide secure public electronic identification (eID), which would include interoperable digital signatures and give EU citizens control over their online identity and related data.

The Commission proposal amends and updates the existing eIDAS Regulation by responding to the challenges raised by its structural shortcomings and limited implementation and to technological developments since its adoption in 2014. The findings of the ex-post evaluation of the eIDAS Regulation shed light on the various limitations preventing the current act from reaching its full potential, while the ex-ante impact assessment of the amending proposal examines the different options, their estimated impact, and the reasoning behind the preferred option. Together, they establish the context for the eIDAS revision, the pitfalls that need to be overcome, and targets.

EU institutions have largely welcomed the Commission proposal in terms of its objectives and concept. However, concerns remain, notably when it comes to finding the right scope for the act, defining the roles and liabilities of various public and private sector actors, ensuring high data protection, and building an inclusive system that leaves no one behind.

### Background to the eIDAS revision

The [eIDAS Regulation](#) ((EU) No 910/2014)<sup>1</sup> introduced the first cross-border framework for trusted digital identities and trust services, providing secure electronic interactions between citizens, business and public authorities. It sought to give EU citizens access to public services across the EU using electronic identification issued in their home country and recognised mutually by other Member States.

According to the Commission evaluation, the eIDAS Regulation has only partially fulfilled the objectives set out in 2014. There remain significant shortcomings, stemming notably from the structure of the act, its limited implementation and the changing technical environment, together with evolving user expectations.

The eIDAS Regulation was introduced in 2014 and has been fully in force since 1 July 2016, and the EU-wide recognition of notified eID schemes started on 29 September 2018.<sup>2</sup> The Regulation mandates the Commission to issue delegated and implementing acts to define technical specifications and to ensure harmonised implementation;<sup>3</sup> thus, its application relies largely on the

enactment of these secondary acts. Standards (ETSI/ISO), recommendations and guidelines from corresponding EU authorities, such as the European Union Agency for Cybersecurity (ENISA), complement the legislative acts in this field. The Regulation covers electronic identification schemes notified by a Member State to the Commission, and to trust service providers established in the EU. Its legal base is Article 114 TFEU, which lays the foundation for removing barriers to the functioning of the single market by approximating Member States' legislation.

In her [State of the Union speech](#) of 16 September 2020, Commission President Ursula von der Leyen presented an initiative for a European digital identity, which would make access to digital services easier across Europe and guarantee people greater control over the data they wish to share. The European Council raised the revision of the eIDAS framework in its [conclusions](#) of 2 October 2020, where it called for the development of an EU-wide framework for secure public electronic identification. It invited the Commission to come forward with a proposal by mid-2021 on an interoperable digital signature giving EU citizens control over their online identity and related data, and enabling access to public, private and cross-border digital services.

The revision of the eIDAS Regulation contributes to digital transformation in the EU. The Commission Communication '[2030 Digital Compass: the European way for the Digital Decade](#)' sets a target for 80 % of EU citizens to be using a digital eID solution by 2030; the [strategy for shaping Europe's digital future](#) envisages a universally accepted public electronic identity. The inter-institutional [Declaration on European Digital Rights and Principles for the Digital Decade](#) addresses eID in the context of online public services, with a commitment to ensure all Europeans are offered an accessible, secure and trusted digital identity with access to a broad range of online services. The EU institutions also commit to protecting the interests of people, businesses and public institutions against cybercrime, including identity theft or manipulation. The [2022 Commission work programme](#) anticipates revising several EU acts thematically related to the eIDAS initiative, such as the [Data Act](#), the [Digital Services Act](#) and the [Digital Markets Act](#), as well as proposing an [EU governments interoperability strategy](#). It mentions the [Data Governance Act](#) and the [cybersecurity package](#) as [priority pending proposals](#).

The Covid-19 pandemic has accelerated the digital transition on all fronts and highlighted the importance of digital identity to support this, as well as the post-pandemic recovery of the European economy. The Recovery and Resilience Facility covers, among other things, investment in digital technologies, such as eID and trust services. Financing of the digital transition is part of the 2021-2027 Multiannual Financial Framework, which includes the Digital Europe programme, and amounts to €7.6 billion (in current prices). It strengthens investment in, for example, digital skills, and supports the digitalisation of businesses and public administrations. Other investment programmes promoting the digital economy include Horizon Europe, for research and innovation, and the Connecting Europe Facility for digital infrastructure.

## Main findings of the evaluation report

The Commission [evaluation report](#) and its accompanying [working document](#) present an overview of progress in implementing and applying the eIDAS Regulation to date. The evaluation report,

### Box 1: Examples of sector-specific eID use

**Banking:** eIDAS-based eID would help financial institutions meet their legal obligations in terms of know-your-customer, anti-money laundering and strong authentication of parties. For example, an account could be opened without a physical meeting. In some EU Member States, eIDs created by banks are valid nation-wide, and in others banks contribute to government eIDs.

**Higher education:** The eIDAS network would allow universities to exchange reliable student identification data seamlessly. For example, the Erasmus+ programme already offers such services for student mobility data.

**Aviation:** eIDAS-based eID would give airlines an adequate basis for cross-border recognition processes. Passengers would not need to have physical passports to share the requested attributes.

Source: Study supporting the Commission ex-post evaluation report on eIDAS Regulation (EU) No 910/2014, which refers to several sector-specific studies.

carried out between September 2019 and December 2020, responds to the review obligation set in Article 49 of the Regulation, which requested an evaluation by July 2020.

## General remarks

Currently, the eIDAS Regulation provides the possibility for EU citizens to use their national eIDs to access online services from other European countries if they belong to the network of notified eID schemes. In principle, [eID issued](#) in one EU country must be [mutually recognised](#) in other Member States if it meets the requirements set in the eIDAS Regulation and has been notified accordingly.

One of the success factors in the Regulation is the number of eID schemes that have been notified, which defines the level of application in practice. A total of 19 eID schemes (including in the UK) have been notified to the Commission by 14 Member States, with some notifying multiple schemes.<sup>4</sup> However, only about 60 % of EU citizens may benefit from cross-border electronic identification services, which is considered a relatively low level of application. As there is no obligation for Member States to notify eID schemes under the 2014 eIDAS Regulation, several Member States have not created one or have chosen not to seek mutual recognition of their national eID schemes.

### Box 2: Five core trust services

**eSignature:** Electronic signature is a legal concept capturing the signatory's intent to be bound by the terms of the signed document.

**eSeal:** Data in electronic form, which are attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

**Electronic time stamps:** Data in electronic form, which bind other data in electronic form to a particular time, establishing evidence that the latter data existed at that time.

**Electronic registered delivery services:** A service to transmit data between third parties by electronic means, providing evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and which protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

**Certificates for website authentication:** Attestation that makes possible authentication of a website and links it to the natural or legal person to whom the certificate is issued.

'Qualified trust service' means that the service meets the applicable requirements laid down in the eIDAS Regulation.

Source: [eIDAS Regulation](#) (EU) No 910/2014.

In trust services, the eIDAS Regulation has contributed positively to the development of an EU internal market on various fronts. One of the main indicators of its impact and application is the steadily rising number of active qualified trust service providers operating in the EU and EEA/EFTA countries. According to the [Trusted List Browser](#), there were 208 active trusted service providers in the EU and EEA/EFTA countries in February 2022 and some 60 trust service providers without active listed services.

In addition to slow application rates in eID, some shortcomings in the existing eIDAS Regulation have become apparent due to technological developments that offer new types of electronic identity solutions, such as electronic ledgers. User expectations have also changed, with smartphones providing smooth, mobile online transactions. Users expect seamless possibilities to share various data attributes online, with a high level of control and security safeguards embedded in the system. The EU legislative landscape has evolved through, for example, the entry into force of the [General Data Protection Regulation](#) (GDPR) in May 2018 and the [EU Digital Agenda 2030](#) in March 2021.

The evaluation report is underpinned by a [study](#) and builds on evidence from various sources, including an open public consultation, targeted stakeholder consultations (surveys, interviews and workshops), and literature review. The [open public consultation](#) on the 2014 eIDAS Regulation, conducted between July and October 2020, asked the respondents, among other things, about the benefits and limitations of the cross-border use of eIDs and trust services.<sup>5</sup> The [Commission working document](#) summarises the results of the consultation and offers insights as to the benefits/limitations that stakeholders associate with the application of the 2014 Regulation.

The consultation reveals that the benefits and limitations in the areas of trust services and eID are largely the same – lack of awareness being the number one limitation and saving time the main benefit of both. Issues related to lack of relevant services, trust and complexity feature high among limitations, while increased legal certainty and simplification of administrative procedures are among the main benefits.

Table 1: Five most cited benefits and limitations of the cross-border use of eIDs and trust services

	Benefits (top 5)	Limitations (top 5)
eID	<ul style="list-style-type: none"> <li>Saving time (77 %)</li> <li>Simplification of administrative procedure (74 %)</li> <li>Increased certainty of the authenticity of user's identity (73 %)</li> <li>Better access to services in other EU countries (72 %)</li> <li>Saving money (68 %)</li> </ul>	<ul style="list-style-type: none"> <li>Lack of awareness (50 %)</li> <li>Limited amount of notified eID schemes (50 %)</li> <li>Lack of relevant public services (47 %)</li> <li>Limited scope of eID schemes notified under eIDAS (43 %)</li> <li>Legal obstacles (e.g. face-to-face interaction required by national legislation) (40 %)</li> </ul>
Trust services	<ul style="list-style-type: none"> <li>Saving time (85 %)</li> <li>Ensuring legal certainty (84 %)</li> <li>Simplification of administrative procedure (77 %)</li> <li>Increase of service security (77 %)</li> <li>Saving money (72 %)</li> </ul>	<ul style="list-style-type: none"> <li>Lack of awareness (50 %)</li> <li>Lack of relevant services (39 %)</li> <li>Complicated/not user-friendly/accessibility barriers for persons with disabilities (36 %)</li> <li>Preference for paper-based solutions or face-to-face interaction (24 %)</li> <li>Lack of trust or fraud concerns (19 %)</li> </ul>

The Regulatory Scrutiny Board (RSB) gave a positive [opinion](#) on the evaluation report, but raised two areas for improvement. First, increased clarity on what success was supposed to look like following the entry into force of the 2014 Regulation and the main driving factors underpinning the shortcomings in the uptake of eID schemes. Second, to deepen the assessment of the continued relevance of the 2014 Regulation, taking into account evolving user needs and technological and market developments.

## Focus on barriers to effective implementation and application

The [evaluation report](#) examined the effectiveness, efficiency, relevance, coherence and EU added value of the 2014 eIDAS Regulation in relation to its implementation and application compared with its objectives, and assessed whether it remains fit for purpose. The main general objectives of the 2014 Regulation include the development of a Digital Single Market and strengthening competition within it while ensuring the interests of consumers. The specific objectives sought to increase cross-sector and cross-border electronic identity services, both public and private; support competitive market development; stimulate the industry and service sectors; ensure an optimal level of governance; and guarantee consumer benefits.

**Effectiveness:** The effectiveness assessment of an EU legal act examines to what extent it has delivered on the expectations and objectives set for it when it was approved. In terms of achievements, the provisions on electronic identity have contributed to the creation of an eIDAS network, which enables holders of a **notified eID** scheme to access online public services across borders. In spite of the limited number of notified eID schemes, interoperability of a number of such eID schemes was ensured within the framework of the eIDAS Regulation, though it is still a challenge on a larger scale.

Despite its achievements, the eIDAS Regulation did not fully meet the expectations set for it. For example, it did not cover the largest part of the identity market due to the low amount of notified eIDs. A lack of incentives for Member States and private service providers to join the cross-border infrastructure constituted one of the major barriers to its effective implementation, contributing to a low number of cross-border use cases.

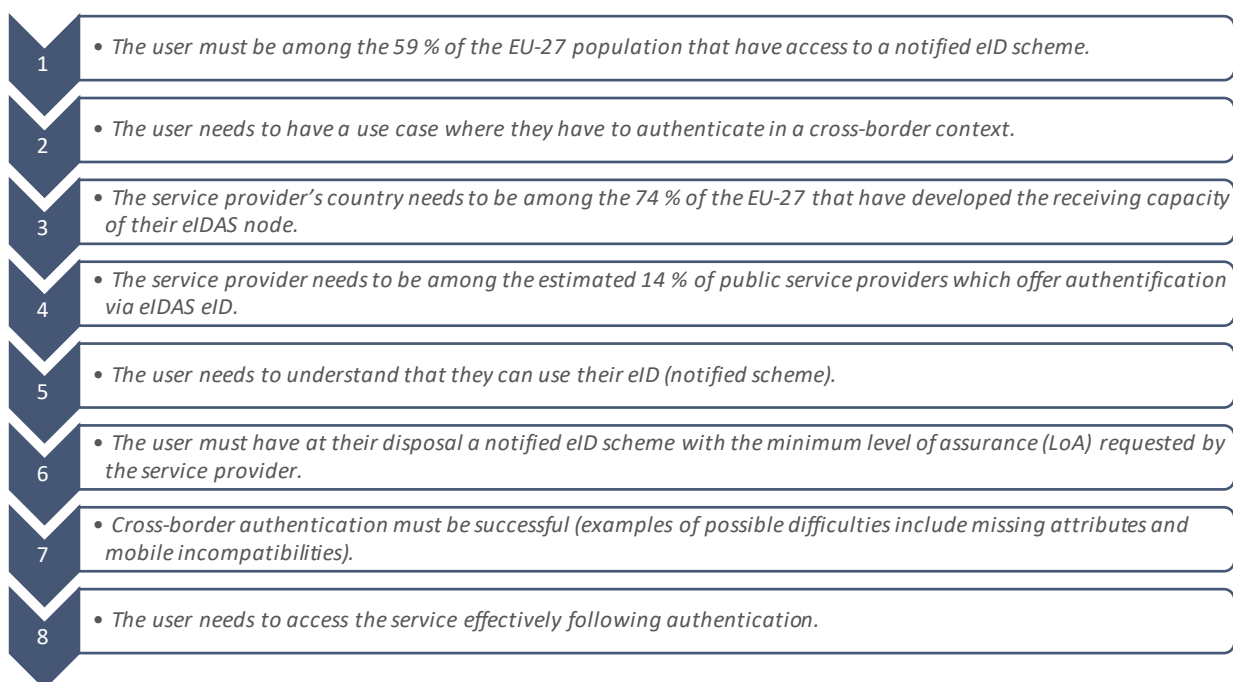
Public e-government applications are necessary to develop usage and to constitute a first user base, but large-scale usage and expansion to a variety of use cases may only be achieved through private-

sector applications. According to the report, only a limited amount of public services offer an eIDAS authentication and only about half of the services accessible through domestic eIDs are part of the eIDAS infrastructure.

The report also raised problems of governance, notably complexity of certification, monitoring and reporting procedures (notification and peer review), as well as a need to clarify security safeguards and incident management. Moreover, the monitoring and reporting obligations are not clear in terms of limiting access to relevant data. Lack of awareness of eIDAS among citizens is another of the main limitations to larger application.

In **trust services**, the eIDAS Regulation has constituted a solid legal framework and, in that context, contributed to legal certainty on liability, burden of proof and legal effect. Despite these successes, some significant shortcomings remain, notably in the area of diverging national interpretations. Numerous delegated and implementing acts, and the work of European and national standardisation organisations, specify and complement the act. It was decided that the eIDAS Regulation should be technology-neutral regarding trust services, the downside of which has been diverging choices in different Member States. Together with slow adoption of implementing acts, it has led to diversity of interpretation at national level, such as varying interpretations by supervisory and conformity assessment bodies.

Figure1: Overview of factors limiting the uptake of the eIDAS eID and its effectiveness.



Source: [Study](#) supporting the Commission ex-post evaluation report on eIDAS Regulation (EU) No 910/2014.

**Efficiency:** The cost-benefit analysis and the cost-effectiveness assessment are at the heart of the efficiency assessment. For the cost-benefit analysis, the report concluded that quantifiable costs have so far exceeded the benefits for both eIDs and trust services, the main factor being the low uptake of the **eID/eIDAS** notified schemes, due to which potential benefits remained hypothetical. For eID, costs and benefits were mainly related to administrative costs derived from managing the system.<sup>6</sup> For **trust services**, accreditation, conformity assessment and supervisory bodies, as well as qualified and non-qualified trust service providers, carried the main costs as well as benefits. From the viewpoint of individual stakeholders, a considerable part of the benefits remained hard to quantify and they had not materialised.

**Relevance:** The Commission examined the objectives of the eIDAS Regulation in relation to the needs, problems and issues at hand, to assess its relevance to current and emerging needs. The profound change the **eID ecosystem** has undergone in recent years points to the need to revise it and influence its actual relevance. Consequently, the evaluation points out that the objective of giving all EU citizens access to a secure and interoperable electronic identity has not been achieved.

However, the original objective remains relevant, i.e. to reduce market fragmentation and to ensure cross-border and cross-sector interoperability of **trust services** by adopting common standards. In terms of issues to revise, the report mentions the limited scope and focus on notified eID schemes for access to online public services. In addition, the vast majority of eID needs are in the private sector, which is not within the scope of the Regulation, and the needs of specific sectors are left outside the existing Regulation.

**Coherence:** Both the internal and external aspects of the Regulation were assessed for coherence. On the positive side, the eIDAS Regulation has increased coherence in its area of application by providing a system of mutual recognition of national eID schemes based on notification and peer review; it is also considered to provide a coherent supervisory system for trust services. Nevertheless, coherence is one of the evaluation criteria where the report finds significant room for improvement. For **eID**, the report revealed practical weaknesses related to implementation of the three levels of assurance (low, substantial and high). Although the Regulation and related implementation acts seek to provide solid notification based on a peer review system, in practice Member States still lack common understanding of what is a substantial or high level of assurance. The report also highlights the limitations of the eIDAS approach to data attributes and their disclosure, which hinders its implementation in a number of use cases, and the lack of provisions for mutual recognition of non EU-based eIDs. Moreover, the eIDAS Regulation's focus on public services, and its rigid approach to the sharing and disclosure of data attributes, limited the use cases and restricted its coherence with other EU acts, such as the GDPR.<sup>7</sup>

For **trust services**, the evaluation report identified some issues to solve in order to maintain a level playing field. The role of conformity assessment bodies should be clarified in terms of their obligations, liability and level of competence; the findings showed differences between national supervisory regimes and varying quality of conformity assessment reports. Moreover, the divergent national approaches in certain areas, such as biometric verification, create uncertainties. These variations could be addressed by developing common standards.

**EU added value:** The evaluation report considered that the eIDAS Regulation fulfilled the criterion of EU added value, since it created an EU-wide harmonised legal framework for **both eIDs and trust services**. Although the impact remained limited due to the low coverage, uptake and usage of electronic identity, it did create incentives for Member States to deploy eID solutions. For trust services, the eIDAS Regulation has reduced fragmentation of the Single Market Regulation and provided legal certainty, thus fostering the uptake of trust services. The option of repealing the eIDAS Regulation would probably reverse its positive effects and lead to more fragmentation of the market, and would influence negatively EU acts related to the eIDAS framework.

## Ex ante impact assessment of the proposal

The Commission [impact assessment](#) (IA) offers an evidence-based, structured analysis of the recognised policy problems and corresponding policy responses by assessing the impact of alternative policy options. The IA also considers subsidiarity, proportionality and future monitoring and evaluation of the policy under scrutiny.<sup>8</sup> The EPRS briefing '[Establishing a framework for a European digital identity](#)' provides a methodological analysis of the IA.

The **intervention logic** builds on the general objective of ensuring the proper functioning of the internal market in the field of cross-border and cross-sector public and private services that rely on highly secure and trustworthy electronic identity solutions. It puts into practice the targets set in the Communication '[2030 Digital Compass: the European way for the Digital Decade](#)' and the strategic objectives set out in the Communication '[Shaping Europe's digital future](#)', pursuing human-centred and sustainable digital policies. Since the introduction of the eIDAS Regulation in 2014, digitalisation of all areas of the society has increased significantly. Consequently, the demand for means to identify and authenticate online and to exchange digital identity information in a trusted and secure environment have triggered a paradigm shift accelerated by the Covid-19 pandemic.

The **problem definition** in the [impact assessment](#) draws attention to the fact that the current eIDAS legal framework relies on national eID schemes and reaches, de facto, only a relatively small segment

of users' electronic identification needs. The IA defines four main shortcomings and seven drivers underpinning them, largely reflecting the key issues mentioned in the evaluation report.<sup>9</sup> According to the IA, the existing regulation:

- 1 Did not meet increased demand by public and private services for trusted identification and exchange of digital attributes.
- 2 Did not meet the current user expectations for seamless and trusted solutions to identify and share attributes across borders.
- 3 Available digital identity solutions were not able to address sufficiently the evolving data control and security concerns.
- 4 For trust services, the scope of the Regulation remained too limited and the lack of a level playing field across the EU hampered development of an internal market. Areas for improvement included national discrepancies on supervision procedures, diverging processes for remote identity proofing, and differences in conformity assessments.

Based on the analysis and conclusions of the evaluation report, and underpinned by its own collection of evidence, the IA defined **general and specific objectives** for the revision of the eIDAS Regulation. These objectives address the regulatory weaknesses and barriers hampering implementation that were revealed in the evaluation report, and take into account the changes in the context of the eIDAS Regulation.

As a conclusion, the general objectives in both 2014 and 2021 include, at their core, the development of a functioning internal market for eID and trust services, though with a different emphasis reflecting their time of publication. The 2014 objectives include stimulating competition and ensuring a high level of consumer protection, as well as increasing the availability of public and private cross-border services. The 2021 objectives aim to meet user expectations and market demands for private and public cross-border eID and trust services, mentioning explicitly the user-centric approach, and to ensure a level playing field for trust services in the internal market.

Table 2: Objectives of the 2014 eIDAS Regulation and its 2021 amending proposal

	eIDAS Regulation 2014, SWD(2012) 135	Amending proposal 2021, COM(2021) 281
General objective	<i>The development of a Digital Single Market; Stimulating and strengthening sustainable competition in the Digital Single Market; To promote the interest of consumers and to ensure high level of consumer protection for all EU citizens and businesses.</i>	<i>To ensure the proper functioning of the internal market, particularly in relation to the provision and use of cross-border and cross-sector public and private services relying on the availability and use of highly secure and trustworthy electronic identity solutions.</i>
Specific objectives	<i>Increase the availability of cross-border and cross-sector eIDAS services and stimulate the take up of cross-border electronic transactions in all sectors (public and private); Ensure an optimal level and scope of governance; Ensure that competitive market developments are stimulated and that technological developments are not hindered in the eIDAS market; Strengthen the competitiveness of the European industry and services sector; Ensure that all consumers can benefit from the advantages of (cross-border) eIDAS services.</i>	<i>Provide access to trusted and secure digital identity solutions that can be used across borders, meeting user expectations and market demand; Ensure that public and private services can rely on trusted and secure digital identity solutions across borders. Provide citizens full control of their personal data and assure their security when using digital identity solutions. Ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.</i>

The three different options presented in the IA rely upon each other, so that the **preferred option** (option 3) includes the main elements of the other options. Option 1 preserves and strengthens the effectiveness and efficiency of the current eIDAS. Option 2 extends the scope of the current framework by establishing an ecosystem for the secure exchange of potentially any data linked to identity. Option 3 would establish a personal European Digital Identity Wallet App system giving users access to public and private online services across borders.

Key elements of option 3 are that: users would be able to carry out transactions online securely in a wide range of use cases; it includes the free flow and exchange of digital identity data across borders, and a strong, trusted way to store and manage identity and share electronic attestations of attributes; it would link the eIDs notified by the Member States to a Wallet App; data protection and user control over identity data are core components; it would also introduce new trust services.

Among the different options analysed in the IA, the preferred option was considered to present the highest level of ambition and to respond in the most effective and efficient manner to the objectives of the revision. As option 3 aims to establish EU-wide secure public electronic identification that gives users control over their online identity, and to enable cross-border access to digital services, it is the only option in full coherence with the European Council's strategic guidelines and the political aims expressed in the 2020 State of the Union speech. It is also aligned with the principles of subsidiarity and proportionality.

According to the [study](#) supporting the IA, the biggest **beneficiaries** of the European personal identity wallet would be citizens/end users. The user-centric design and mobile-first thinking, and the procedures to establish common standards, are expected to contribute to a consistent and accessible user experience. A privacy-by-design approach is envisaged to allow citizens to communicate directly with providers of services and credentials, while simplified identity management would allow sharing of identity credentials received from various sources to anywhere in the EU. Increased security and the proposed certification systems would reduce the likelihood of fraudulent behaviour. Other benefits include reduced operating costs for online service providers and new market opportunities for Wallet App providers. The **main costs** are envisaged to fall on public authorities, such as costs of supervision and costs associated with the development of standards. Wallet App providers would face first-time development costs and on-boarding costs for both credential providers and service providers, for example.

## Main features of the Commission proposal

The EPRS briefing '[Updating the European digital identity framework](#)' offers an insight into the proposal, follows the legislative procedure and is regularly updated. The following sections take stock of developments as of February 2022.

The [June 2021 amending proposal](#) builds upon the existing system of a cross-border legal framework for trusted electronic identification of natural and legal persons and trust services, but aims to enlarge its scope from relying on national digital identity schemes to electronic attestations of attributes that are valid at European level. Member States would [provide](#) citizens and businesses with digital wallets capable of linking their national digital identities with proof of other personal attributes. Such wallets could be issued either by a Member State, under a mandate from a Member State, or independently but recognised by a Member State.

**Technical implementation** work has started simultaneously with the legislative process, guided by a [recommendation](#) on a toolbox procedure issued together with the amending proposal. The **toolbox** establishes a structured process that supports the implementation of the European Digital Identity Framework, based on cooperation between Member States, the Commission and other stakeholders. The [eIDAS expert group](#) acts as the main interlocutor, while a standardisation body – the European Telecommunications Standards Institute (ETSI) – relevant private and public sector stakeholders and external experts are also consulted and associated with the work. The toolbox is expected to produce a number of implementing acts defining a technical architecture and reference framework; a set of common standards and technical specifications; common guidelines and best practices to support the smooth functioning of the European Digital Identity Framework. Its scope covers all aspects of the functionality of the Digital Identity Wallet and of the qualified trust services for attestation of attributes, and its results will be adapted as necessary to the outcome of the legislative process. The Recommendation envisages publication of the toolbox by October 2022.

**The proposal envisages** a requirement for each Member State to issue a European Digital Identity Wallet within 12 months after the Regulation's entry into force. The notification of at least one electronic identification scheme is proposed to be mandatory.



A compulsory compliance assessment and a voluntary cybersecurity certification, as established by the [Cybersecurity Act](#), would ensure compliance. In addition, specific provisions would be applicable to the 'relying parties' regarding prevention of fraud and authentication of personal identification data and digital attestations of electronic attributes. For citizens, the wallet would be free and voluntary.

According to the proposal, the security and user-centric control offered by the updated European Digital Identity Framework would give everyone the means to control their digital ID regarding who has access and to which data exactly, and to decide on its disclosure. This entails a high level of security for all aspects of digital identity, including the issuing of a European Digital Identity Wallet, and the infrastructure for the collection, storage and disclosure of data. In situations where authentication of a person is required by law, the proposal suggests unique identification of natural persons. To this end, Member States are requested to include in the minimum set of person identification data a unique and persistent identifier to identify the user upon their request in cases where the law obliges identification. A certification of conformity issued in accordance with a relevant European cybersecurity certification scheme would ensure a high level of trust and interoperability. In addition, the proposal establishes strict requirements for data protection and privacy for the issuer of the European Digital Identity Wallet and for qualified providers of attestations of attributes, including compliance with GDPR requirements.

The proposal would enlarge its scope to three new areas: electronic archiving and electronic attestation of attributes, the management of remote electronic signature and seal creation devices, and electronic ledgers. The European Digital Identity Wallet would include the official identity data, as issued by Member States, and other identity attributes as electronic attestations of attributes. Website authentication allows users to identify who is behind a specific website; the proposal would require providers of web browsers to facilitate the use of qualified certificates for website authentication. The compliance aspects of the European Digital Identity Wallet with these requirements rely on certifications provided by accredited public or private-sector bodies designated by Member States. On the international aspects of trust services, the draft proposal gives the Commission a mandate to act in terms of attesting the equivalence of requirements applied to services established in third countries. Finally, the revision proposes a new article on collecting statistical information on the use of the European Digital Identity Wallet, with a view to monitoring the performance of the Regulation.

## Views of the European Data Protection Supervisor (EDPS)

On 28 July 2021, the European Data Protection Supervisor (EDPS) gave [formal comments](#) on the Commission proposal amending the eIDAS Regulation. The EDPS welcomed the general approach to build on the existing legal act, enhance EU added value and increase harmonisation of the EU-level framework on digital identity and trust services. However, the EDPS noted that the technical implementation of the act will take place through secondary legislation. Thus, compliance of the amended eIDAS with the [GDPR](#) cannot be fully assessed before the implementing acts laying down the technical specifications and reference standards are in place.

On the specific provisions of the proposal, the EDPS: appreciates clarification on the use of electronic ledgers, which are restricted to specific-use cases; notes the service provider's compliance duty regarding the use of electronic ledgers, and mentions blockchain technology as an area where additional safeguards may be needed;<sup>10</sup> supports the empowerment of the data subject, since it gives EU citizens more transparency over their personal data and better control regarding with whom and for what purpose it is shared; praises the principle of data minimisation, as it explicitly prohibits the issuer of the European Digital Identity Wallet from collecting information about the user to the minimum necessary; welcomes the mandatory certification procedure of certain requirements for European Digital Identification Wallets; recommends finding alternative ways to replace the proposed unique and persistent identifier, as it might cause problems with the GDPR and some national jurisdictions.

On monitoring and supervision, the EDPS draws attention to the GDPR, which requires action from those in control functions no later than 72 hours after having become aware of a qualified data

breach. The EDPS also draws attention to the use of personal data by providers of services for qualified or non-qualified electronic attestation of attributes, underlining the importance of increasing trust in the system and preventing misuse of data. It further notes that the GDPR provision that prohibits combining personal data from the above-mentioned sources with personal data from different types of services cannot be circumvented by contractual clauses or consent.

## European Parliament views

The Committee on Industry, Research and Energy (ITRE) is the main committee handling the revision of the eIDAS Regulation, with Romana Jerković (S&D, Croatia) as the rapporteur. On 3 February 2022, ITRE held a [public hearing](#) on the European Digital Identity Wallet and Trust Services. The committee heard panellists and [discussed](#) the impact of the amending proposal on the protection of personal data, cybersecurity, and interoperability and usability of trust services. They also exchanged views on the role of public and private actors regarding the Digital Identity Wallet.

Three European Parliament own-initiative resolutions on the Digital Services Act (DSA), of which two are legislative initiatives, address the role of EU-wide electronic identification and offer insights into Parliament's views in a larger context. Trusted and secure electronic identification is seen as fundamental to ensuring access to digital services and essential for developing the data economy.

## European Parliament own-initiative resolutions

On 20 October 2020, the Parliament adopted two legislative-initiative resolutions with recommendations to the Commission on the Digital Services Act. In the [resolution](#) on 'Improving the functioning of the Single Market', the Parliament refers directly to the revision of the eIDAS Regulation, while in [the other](#) it does not address this topic. Parliament underlines the need to improve efficiency of electronic interactions between businesses and consumers. It considers the update of the eIDAS Regulation a necessity to ensure the efficiency of the DSA and supports the development of a universally accepted, trusted digital identity that would apply to natural persons, legal entities and machines. In this context, Parliament also highlighted the principle of data minimisation (under the GDPR), which prohibits the collection of unnecessary data. In addition, Parliament called on the Commission to assess the possibility of establishing an age verification system for users of digital services, to protect minors.

In its [resolution](#) on the Digital Services Act and fundamental rights issues, Parliament reminded the Commission about the low level of notified electronic identity schemes and emphasised the importance of a trusted and secure electronic identification system to the development of digital services. It also stressed the principle of data minimisation and referred to the collection of unnecessary personal data by online platforms, often caused by the use of single sign-in possibilities. Parliament recommended that online platforms with a dominant market share and supporting a single sign-in service should be required to support at least one open identity system based on a non-proprietary, decentralised and interoperable framework.

## Selected parliamentary questions

On [16 June 2021](#), Carles Puigdemont i Casamajó (NI), Antoni Comín i Oliveres (NI) and Clara Ponsatí Obiols (NI) tabled a written question to the Commission on the European Digital Identity and existing regional and national eIDAS schemes. They enquired whether the proposal is compatible with existing national or regional digital identity frameworks and referred to the Catalan Government's eID scheme. They also addressed the possible use of distributed ledger technology in developing a European eID and what safeguards the system would offer for users. In his [answer](#) of 17 August 2021, Commissioner Breton explained that the proposal builds on Member States' notified national electronic identity and mentioned that the proposal is technology-neutral. The toolbox procedure is in place to define the technical architecture, common standards, and best practices and guidelines for the European Digital Identity Framework. As regards guarantees for users, he said that the proposal is aligned with data protection and privacy rules.

On [8 September 2020](#), Dita Charanzová (Renew) asked the Commission whether it plans to establish a single sign-in system in the context of the eIDAS revision and how it plans to assess the possible impacts of such an action. Commissioner Breton [answered](#) on 20 October 2020 and provided information about an ongoing impact assessment covering various policy options underpinning the eIDAS revision. The options under consideration seek to promote the wider use and acceptance of electronic identities and would allow EU citizens to access online public and private services. The Commission pointed out that the impact assessment built on the evaluation of the implementation and application of the 2014 eIDAS Regulation and mentioned the supporting public consultation that ran from 24 July until 2 October 2020.

## Council of the European Union

At the time of writing, the Council is drafting conclusions on the Commission's proposal for a European Digital Identity under the French Council Presidency. However, the discussion held in the [Telecom Council](#) of 3 December 2021 offers an insight into their views. Ministers took note of a [progress report](#) summarising the work within the Council up to November 2021. According to the report, Member States received the proposal positively and praised its level of ambition. Nevertheless, delegations raised concerns over the proposed deadline to introduce an ID scheme within 12 months of the entry into force of the Regulation; the proposed provisions on a unique and persistent identifier; the interaction between the eIDAS and the GDPR; the Single Digital Gateway; the once-only principle of the e-government sector; and cybersecurity. Moreover, Member States discussed the proposed certification of the eID schemes. The delegations also flagged that the lack of sanctions in case of non-compliance might influence the enforcement of the Regulation in practice; underlined the importance of respecting the competence structure of national authorities and national policies in relation to attestation of attributes; and highlighted that data collection for statistical purposes could create additional administrative burdens for national authorities.

## European Economic and Social Committee

The European Economic and Social Committee (EESC) adopted an [opinion](#) on European electronic identification on 20 October 2021. It welcomes the Commission proposal and supports the user-centric approach that allows users control over their own data, possibilities to determine access to data and to choose what information is shared. Furthermore, the EESC supports actions to enhance inclusion, such as technological skills development for elderly users and other vulnerable groups. The EESC draws attention to the need to align national legislation and EU-level acts regarding qualified electronic attestation of attributes. It sees the protection of personal data in the context of fundamental rights, and thus emphasises the importance of the right to privacy and right to protection of personal data. The Committee raises security concerns over data fraud related to the digitalisation process, especially the development of an EU-wide system that stores and processes data. In addition, the EESC argues that users of Digital Identity Wallets should be guaranteed compensation in situations of data loss or fraudulent behaviour and that this liability should be independent of whether the provider is at fault.

## Committee of the Regions

The Committee of the Regions (CoR) welcomed the Commission proposal in its [opinion](#) on the European Digital Identity, adopted on 12-14 October 2021. It raised concerns about a hasty implementation of a European Digital Identity Wallet solution by drawing attention to the technical risks involved in creating centralised storage of identity data. The CoR underlined the importance of adequate safeguards against IT threats, data breaches and possible cyber-attacks, and suggested that the authorisation check for eID access for economic operators should be based on a secured certificate with limited duration and subject to a regular renewal process. According to the CoR, use of the European Digital Identity Wallet should be voluntary and implementation of the new system should ensure that vulnerable groups, such as the elderly, develop adequate skills. Moreover, it argues that the Regulation should include provisions on the protection of minors in general. The

CoR supports an incremental approach towards implementation, since some areas of the economy and some actors will be involved for the first time with the use of electronic identities.

## MAIN REFERENCES

Negreiro, M., [Updating the European digital identity framework](#), EPRS Briefing, October 2021.

Tuominen, M., [Establishing a framework for a European digital identity](#), EPRS Briefing, October 2021.

[Evaluation study of Regulation No 910/2014](#), European Commission, Directorate-General for Communications Networks, Content and Technology, August 2021.

## ENDNOTES

- <sup>1</sup> [Regulation](#) (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- <sup>2</sup> EurLex does not [inform](#) about infringements of the eIDAS Regulation (EU) No 910/2014 referred to the European Court of Justice. As regard preliminary rulings, one case is [pending](#) in the ECJ.
- <sup>3</sup> Main implementing acts for eIDs: Commission (EC) Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for Member State cooperation on eID; EC Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework; EC Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means; EC Implementing Decision (EU) 2015/1984 of 3 November 2015 on defining the circumstances, formats and procedures for notification.
- <sup>4</sup> Belgium, Italy, the Netherlands and Portugal have notified two or more eID schemes. In addition, three countries had pre-notified schemes by April 2021. For more details, see Commission CEF [website](#) on eID documentation.
- <sup>5</sup> The consultation received 318 contributions, of which 36.48 % were from EU citizens, 30.8 % from companies or business organisations, 10.69 % from business associations, and 8.81 % from public authorities.
- <sup>6</sup> Costs derived from the notification process of eID schemes, the peer review process and the cooperation and communication activities between Member States and the European Commission.
- <sup>7</sup> [Regulation](#) (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data entered into force on 25 May 2018. According to the GDPR principles of 'privacy by default' and 'privacy by design', the exposure of identity attributes should be limited to what is necessary for receiving a certain service.
- <sup>8</sup> For the IA, the Commission collected feedback from a number of stakeholders in the context of the formal meetings with the Member States and in targeted bilateral meetings with private and public stakeholders. The open public consultation, desk research, expert interviews, focus groups and workshops also contributed to the evidence base; the IA was also supported by a study. SWD(2021) 124 explains in detail the methods and models used for impact assessments.
- <sup>9</sup> The RSB [opinion](#) gave, first, a negative assessment and then, on a second reading, a positive assessment on the impact assessment. One of the remaining shortcomings was the definition of the evolving situation and its drivers and their common impact on the needs of the revision.
- <sup>10</sup> Data Protection Board guidelines on block chain – [EDBP work programme 2021/2022](#).

## DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2022.

[eprs@ep.europa.eu](mailto:eprs@ep.europa.eu) (contact)

[www.eprs.ep.parl.union.eu](http://www.eprs.ep.parl.union.eu) (intranet)

[www.europarl.europa.eu/thinktank](http://www.europarl.europa.eu/thinktank) (internet)

<http://epthinktank.eu> (blog)

