BRIEFING

EU Legislation in Progress

European Parliament

Updating the European digital identity framework

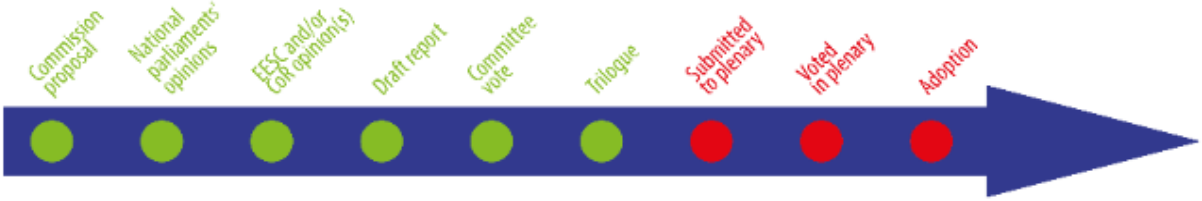
OVERVIEW

The 2014 Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation or eIDAS) was the first digital identity legislation to pave the way for cross-border electronic identification, authentication and website certification across the EU. While the application of eIDAS has had a mixed record, the pandemic has fuelled demand for eIDAS solutions that are capable of ensuring broader access to public and private services.

On 3 June 2021, the European Commission put forward a proposal to update the European digital identity framework. This would allow citizens across the EU to identify and authenticate themselves online (through their European digital identity wallet), share digital documents or prove a specific identity attribute such as age. In parallel, the Commission adopted a recommendation to design a toolbox supporting the framework so as to avoid fragmentation and barriers due to diverging standards.

After the European Parliament and the Council of the EU approved their negotiating positions on the proposal in March 2023 and December 2022 respectively, they reached a provisional agreement on the creation of a pan-European digital identity framework on 8 November 2023. Both now need to formally adopt the text before it is published in the Official Journal of the EU and enters into force.

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		
Committee responsible:	Industry, Research and Energy (ITRE)	COM(2021) 281 3.6.2021 2021/0136(COD) Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
Rapporteur:	Romana Jerković (S&D, Croatia)	
Shadow rapporteurs:	Riho Terras (EPP, Estonia) Alin Mituța (Renew, Romania) Mikuláš Peksa (Greens/EFA, Czechia) Paolo Borchia (ID, Italy) Robert Roos (ECR, the Netherlands) Elena Kountoura (The Left, Greece)	
Next steps expected:	Final first-reading vote in plenary	



EPRS | European Parliamentary Research Service

Authors: Mar Negreiro and Maria Niestadt
Members' Research Service

PE 698.772 – January 2024

EN

Introduction

Since the onset of the coronavirus pandemic, the provision of public and private services has become increasingly digital. Digitalisation can allow continued provision of what are often vital services (for example, in healthcare). This rapid digitalisation of services has inevitably increased demand for the digital provision of credentials, such as means for users to identify and authenticate themselves online. Governments and businesses alike need to adapt and serve customers and citizens digitally. However, access to public services and certain sectors (healthcare, finance, etc.) requires identification or the exchange of attributes[1] with a high level of security and trustworthiness, including in terms of data protection. While secure identification systems are sometimes mandated by law, there is also increased demand for them, as most EU citizens would like access to a secure digital identity to use for online services. Moreover, according to Europol, online fraud schemes, among them identity theft, are a major crime threat in the EU.

Digital identity provision is undergoing fundamental changes. Entities such as banks, electronic communication service providers and utility companies, some of which are required by law to collect identity attributes, are leveraging their procedures to act as verified identity providers. There are many examples of European organisations using verified identities for their online services. Many of these identity verification solutions have been developed by banks, particularly in Scandinavian countries. Nevertheless, many of these solutions are limited to national use and not available across the EU. Similarly, internet intermediaries, including major social media platforms and internet browser companies, also provide their users with digital identity services, mainly in the form of digital wallets.

According to Eurostat, in 2023, 90.3 % of individuals in the EU-27 were regular internet users (i.e. using the internet at least once a week), and about 70 % ordered or bought goods or services over the internet for private use. With increased connectivity, mobile internet users also demand convenience and user-friendliness, including mobile-based digital identity solutions. Existing digital wallet solutions are typically linked to payment solutions (ApplePay, GooglePay, etc.) and allow users to store and link data in a single seamless environment on their mobile phones. However, some critics argue that this convenience comes at the cost of loss of control over the personal data that are being disclosed, while at the same time these solutions are disconnected from a verified physical identity, which, according to the European Commission, makes fraud and cybersecurity threats more difficult to mitigate.

Against this backdrop, the Commission put forward a proposal for a regulation on a framework for a European digital identity (EU eID) in 2021.

Existing situation

The Commission's initiative builds on the Regulation on European electronic identification and trust services (eIDAS Regulation, or eIDAS for short). Adopted in 2014, the regulation paved the way to cross-border electronic identification, authentication and website certification within the EU. Before the regulation entered into force, there was no comprehensive EU cross-border or cross-sector framework for electronic identification (eID), authentication and trust services capable of ensuring secure, trustworthy and easy-to-use electronic transactions. However, the 2014 regulation has some limits. It is based on national eID systems that follow varying standards and focuses on a relatively small segment of the electronic identification (eID) needs of citizens and businesses, namely secure cross-border access to public services. Moreover, the regulation does not require EU Member States to develop a national digital ID and to make it interoperable with those of other Member States, which leads to large discrepancies between countries. Last but not least, the regulation has no provisions on the use of such identification for private services or mobile terminals, which again leads to differences between countries.

At present, demand cannot be met by the eID means and trust services regulated by eIDAS, given its current limitations. Meanwhile, identification and authentication means developed by the private sector outside the eIDAS framework can only go so far in responding to the challenge. User-friendly third-party authentication services (for instance, using a Facebook or Google account to log into different services) are common for accessing unregulated private online services that do not require a high level of security, but they cannot offer the same level of legal certainty, data protection and privacy, mainly because they are self-asserted and do not provide a link to trusted and secure government eIDs.

The report of the Commission's expert group on regulatory obstacles to financial innovation (ROFIEG) and the reports of the expert group on eID and know-your-customer (KYC) processes, all published in December 2019, recognised that national regulatory bodies across the EU have different standards regarding the compliance of technical solutions for digital identity verification.

On 9 March 2021, the Commission presented its vision for Europe's digital transformation by 2030. Its communication on the 2030 Digital Compass: the European way for the Digital Decade, sets a number of targets and milestones that the European digital identity would help achieve. For example, by 2030, all key public services should be available online, all citizens should have access to their electronic medical records, and 80 % of citizens should use an eID system.[2] The March 2021 communication builds on the 2020 strategy on shaping Europe's digital future, which remains the overarching framework. In December 2021, the Commission published its proposal to establish the Path to the Digital Decade policy programme, whose goal would be to ensure that the targets are met. The Council and the Parliament reached a provisional agreement on this policy programme in July 2022 (the final act was published in the Official Journal of the EU in December 2022). The same message was reinforced by the European declaration on digital rights and principles (signed in December 2022), which envisages that 'people living in the EU are offered the possibility to use an accessible, voluntary, secure and trusted digital identity that gives access to a broad range of online services'.

Parliament's starting position

In its October 2020 resolution on the digital services act and fundamental rights issues, Parliament highlighted that, while trusted electronic identification is 'elementary in order to ensure secure access to digital services and to carry out electronic transactions in a safer way', only about half of Member States have notified the Commission of their electronic identity schemes for cross-border recognition under the eIDAS Regulation. Parliament also stressed the unnecessary collection of personal data, such as mobile phone numbers, by online platforms at the point of registration for a service, often caused by the use of single sign-in possibilities. It underlined that the General Data Protection Regulation (GDPR) clearly describes the data minimisation principle,[3] and recommended that online platforms that support a single sign-in service with a dominant market share should be required to also support at least one open identity system based on a non-proprietary, decentralised and interoperable framework.

Council and European Council starting position

In its conclusions of 1-2 October 2020, the European Council asked the Commission to introduce an EU-wide framework for secure public eID (European digital identification) by mid-2021. Similarly, reaching a general approach on the proposed regulation on a European digital identity framework has been high on the agenda of successive Member States holding the presidency of the Council.

Preparation of the proposal

In line with the requirement set in Article 49 of the 2014 eIDAS Regulation, in 2020 the Commission reviewed the extent to which the eIDAS framework remained fit for purpose and delivered the intended outcomes, results and impact. It also considered whether it is appropriate to modify the

scope of the regulation or its specific provisions, taking into account the experience gained in its application as well as technological, market and legal developments. As part of the review, the Commission carried out an evaluation of the eIDAS framework, commissioned an external study, performed an impact assessment and conducted an open public consultation, among other things. The results of these are described below.

Evaluation

The evaluation of the eIDAS framework revealed that the 2014 eIDAS Regulation falls short of addressing new market demands. As mentioned above, the regulation builds on Member States' national electronic identity schemes notified under eIDAS, but as it does not require Member States to develop their national digital IDs or make them interoperable with those of other Member States, this has led to large discrepancies between the Member States. Although the regulation has delivered on many of its goals and has become a fundamental element in facilitating the single market in a number of sectors (more specifically by facilitating financial services and enabling access and reuse of data in administrative procedures), it comes with a number of limitations. These include the lack of an obligation to notify national eID schemes, the limited attributes that can be reliably disclosed to third parties, the act's focus on the public sector, and the absence of clear incentives for private parties to use national eIDs. In addition, the evaluation found that the European electronic identity ecosystem is distributed across different national regulatory environments, levels of digital governance, cultures and levels of trust in public institutions.

Impact assessment and study

On 23 July 2020, the Commission published an inception impact assessment with details of its plans to review the 2014 eIDAS Regulation. It concluded that the potential of electronic identification and authentication under eIDAS remains under-exploited.

On 3 June 2021, the Commission published a study on the review of the eIDAS Regulation. This study supports the conclusions drawn in the Commission's impact assessment (IA) in assessing the impact of different policy options to review the regulation, with the aim of establishing an updated legislative framework that is fit for purpose. The study took into consideration the input to the open public consultation conducted from 24 July to 2 October 2020 (see section below).

The study helps to define the problem, the policy options and the justification of the need for EU legislative intervention in this area, and provides a comparative analysis of the costs and benefits expected for the stakeholders affected by the various policy options, namely: public authorities, online service providers, conformity assessment bodies, trust service providers, eID providers and wallet app providers.

The IA identifies three policy options. Under the baseline scenario (option 0), the Commission would not propose any changes to the current legislation, and the eIDAS Regulation and its framework would therefore remain in force. To allow consistent assessment and comparison of the options, the baseline also integrates the measures envisaged under secondary legislation that could be enforced without any changes to the regulation (e.g. implementing acts) or positive spill-overs stemming from other pieces of legislation (such as the Digital Markets Act).

Option 1 involved creating a European digital identity in the form of a strengthened legislative framework for national eIDs notified under eIDAS. It would require Member States to make eIDs available to all citizens and companies for cross-border use, and improve the effectiveness and efficiency of mutual recognition. The use of national eIDs by private online service providers would be triggered and facilitated through harmonised cost and liability rules, extended data sets and access obligations. These measures would be taken without extending the scope of the eIDAS Regulation or affecting its underlying principles (i.e. they would be applicable to eID solutions notified by Member States, but also to mutual recognition and technological neutrality).

Under option 2, the private sector would support the delivery of a European digital identity ecosystem in the form of a new qualified trust service for the exchange of digital identity attributes across borders, such as proof of age (e.g. for accessing age-restricted social media), professional qualifications (e.g. lawyer, student, doctor), digital driving licences and medical test certificates.

Option 3 would define a legal and technical framework for the deployment of the European digital identity as a user-controlled digital wallet app. The wallet app would empower users to securely share data related to their identity with public and private online service providers through their mobile devices. It would also allow them to control their own personal data. Further to legal requirements, common standards and/or technical references for the wallet app would be developed through close dialogue with Member States and private-sector stakeholders.

The IA concluded that option 3 stood out as the preferred one. According to the EPRS initial appraisal, the IA provides a good description of the options' main elements.

The Regulatory Scrutiny Board (RSB) gave a positive opinion on a draft version of the IA report. However, the RSB considered that the IA did not provide a sufficiently clear explanation of the comparison between the policy options regarding their efficiency and effectiveness. Nor did the IA present adequately the views of the various stakeholders.

Public consultation

As part of its review, the Commission also conducted an open public consultation from 24 July to 2 October 2020. The aim of the consultation was to gather feedback on drivers for and barriers to the development and uptake of trust services and eID in Europe. The consultation received responses from a total of 318 stakeholders. A large majority of respondents (60 %) said that they would gladly welcome the creation of a single and universally accepted European digital identity scheme, complementary to the national publicly issued electronic identities. For 57 % of respondents, the complexity involved in the set-up and governance of a single and uniform European digital identity scheme was the main possible disadvantage. The overlap with existing solutions (49 % of respondents) and the lack of flexibility to adapt to technological developments and changing user needs (48 % of respondents) were also considered to be possible disadvantages.

The changes the proposal would bring

On 3 June 2021, the Commission published its proposal on a European digital identity framework based on the revision of the current one. With the proposal, the Commission hopes to meet the objectives of its digital compass, which stipulates that by 2030 all key public services are to be available online and all citizens are to have access to their digital medical records and to a digital ID.

Furthermore, the Commission expects that the security and control offered by the updated European digital identity framework will offer everyone the means to control who has access to their digital ID and to what specific data. This will also require a high level of security with respect to all aspects of digital identity provisioning, including the issuing of a European digital identity wallet and the creation of an infrastructure for the collection, storage and disclosure of digital identity data. The proposal's specific objectives are to:

- 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 with full control of their personal data and ensure their security when using digital identity solutions;
- ensure equal conditions for the provision of qualified trust services in the EU and their acceptance.

The proposed framework for a European digital identity aims to achieve a shift from reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid at European level. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules, and public administrations should be able to rely on electronic documents in a given format.

The Commission proposes to address the shortcomings identified (in the Section on the 'Existing situation'), by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use. It envisages a requirement for each Member State to issue a European digital identity wallet within 12 months after the regulation's entry into force. European digital identity wallets should be issued by a Member State, under a mandate from a Member State, or independently but recognised by a Member State. Thus, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (such as driving licence, diplomas or bank account). These wallets could be issued by public authorities or by private entities, provided these are recognised by a Member State.

The proposal does not impose any particular technology. The proposed European digital identity wallet would include the official identity data as issued by Member States and other identity attributes as electronic attestations of attributes. Article 6a of the draft regulation requires Member States to follow compulsory compliance assessment and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act.

Furthermore, the proposal lays down in Article 6a(7) that the user should be in full control of the wallet, and sets strict requirements for data protection and privacy for the issuers of the European digital identity wallet and for qualified providers of attestations of attributes, including compliance with GDPR requirements. Moreover, to ensure that users can identify who is behind a website, the proposal introduces a new requirement for providers of web browsers to facilitate the use of qualified certificates for website authentication (QWACs), by displaying the QWACs in a user-friendly manner. The conformity of European digital identity wallets with these requirements should be certified by accredited public or private-sector bodies designated by Member States. By relying on a certification scheme based on the availability of standards commonly agreed among Member States, it should be possible to ensure a high level of trust and interoperability.

In parallel, the Commission adopted a recommendation so as to avoid fragmentation and barriers due to diverging standards. This recommendation sets out a process to support a common approach allowing Member States and other stakeholders from the public and private sectors, in close coordination with the Commission, to work towards the development of a toolbox. To meet the 12-month deadline for a European digital identity wallet to be issued in each Member State, this toolbox would accelerate the work by defining the technical architecture, common standards, and best practices and guidelines for the European digital identity framework.

Budget

The Commission supports the implementation of the European digital identity framework through the Digital Europe programme, and many Member States have planned projects for the implementation of the e-government solutions they are required to put in place, including the European digital identity, in their national plans under the Recovery and Resilience Facility. According to the Commission, the total financial resources necessary for the implementation of the proposal in the 2022-2027 period will amount to €30.8 million, including €8.8 million in administrative costs and up to €22 million in operational spending covered by the Digital Europe programme. The financing will support costs linked to maintaining, developing, hosting, operating and supporting the eID and trust services' building blocks. It may also support grants for connecting services to the European digital identity wallet ecosystem, and the development of standards and technical specifications.

The Commission has already co-financed pilot projects under the Digital Europe programme, testing the wallet in a diverse range of everyday use cases such as when filing taxes, opening a bank account, signing contracts or claiming medical prescriptions.

Advisory committees

The European Economic and Social Committee (EESC) adopted an opinion on the proposal during its plenary session on 20-21 October 2021 (rapporteur: Tymoteusz Adam Zych, Diversity Europe – Group III, Poland). The EESC highlights that the proposed digitalisation of services may result in the exclusion of parts of European society, in particular older people, those with low digital literacy and people with disabilities. It also notes that effective data protection needs to be considered in the context of the protection of fundamental rights, particularly the right to privacy and the right to the protection of personal data.

The EESC agrees with the requirement that the European digital identity framework should give users the means to control who has access to their digital ID and what data can be accessed. At the same time it raises security concerns regarding the risks inherent in developing massive centralised systems that store and process sensitive data vulnerable to fraud and loss. The EESC therefore considers that users of European digital identity wallets should be guaranteed compensation for any undesirable situation relating to their data (e.g. data theft or disclosure).

The European Committee of the Regions (CoR) adopted an opinion on the proposal on 13 October 2021 (rapporteur: Mark Weinmeister, EPP, Germany, ECON and NAT commissions). Among other things, the CoR calls for the wallet to be usable worldwide as a proof of EU identity, and to include features such as an official EU vaccination certificate or a digital deposit for visas. The CoR is, however, concerned about the security and technical risks posed by the centralised storage of identity data in a mostly mobile application. It therefore considers it important that the digital identity wallet be sufficiently reinforced against cyber-attacks. When it comes to economic accessing the ID, the authorisation check should be designed with a secured certificate whose validity is of limited duration or is cyclical. The CoR also asks for an extension of the implementation deadline for Member States from 12 to 24 months.

National parliaments

The proposal was open to review by the Member States' national parliaments.

The deadline for the submission of reasoned opinions on grounds of subsidiarity was 4 October 2021. No reasoned opinions were submitted.

Stakeholder views[4]

Stakeholders have been divided in their reactions to some issues. A selection of views expressed in the position papers during the open public consultation is provided below.

Apple supports the objective of ensuring a common approach and technical architecture for EU digital identity wallets. It urges the relevant European institutions to push for the adoption of international standards as common standards for the EU digital identity framework and toolbox.

The Technical Committee on Electronic Signatures and Infrastructures (ETSI TC ESI) in France considers that this legislative proposal, the GDPR, the NIS2 Directive and the Digital Markets and Digital Services Acts impose some security and transparency requirements on providers as well as the obligation to notify certain events that need coordination between the different supervision schemes, in order to avoid duplication that might generate doubt about which technical standards have to be followed.

The City of Stockholm emphasises that it is currently difficult for users to assess how their personal data will be used and what conditions apply, as well as to fully understand the regulations and

conditions within this area. Moreover, it is not clear how the browser developers will be persuaded to comply with the new requirements and accept the new certificates. The City of Stockholm also highlights that the timeline for the proposal has to be realistic.

Microsoft refers to the need to coordinate existing and future EU legislation, such as the NIS2 and the Cybersecurity Act (e.g. regarding certification), to avoid regulatory overlap and inconsistencies.

Finance Denmark sees a risk of fragmentation of public/private solutions. To require private corporations to accept digital identity wallets for authentication purposes means that financial institutions will have to make significant investments. Finance Denmark therefore proposes a solution based on ID switching: the eID would be the identification tool for online onboarding, while authentication for financial services would be based on a digital identity in a format that the individual bank supports.

The Certification Body of Deutsche Telekom Security GmbH states that differing requirements leading to a distribution of responsibilities will probably result in different levels of service-security and service-assurance across the EU. They suggest putting an entity in charge at EU level (such as the EU Agency for Network Information Security, ENISA) with binding effect, to ensure harmonised interpretation and implementation of the amended eIDAS Regulation throughout Europe.

The European Digital SME Alliance recommends making the publication of implementing acts with references to standards mandatory. It also recommends introducing common rules for remote identification, so as to ensure a common approach to security and interoperability and to provide certainty for small and medium-sized companies to invest in eIDAS value-added services.

Eurosmart calls on the Commission to publish a new standardisation request on digital identity to support this proposal. Standards on digital identities are critical and should be developed in a fully transparent manner. According to Eurosmart, the European standardisation approach to digital identity has to prevent some players from diverting the primary objectives of keeping personal data under citizens' control and watering down the 'security-by-design' principle.

Global identity verification provider Onfido is worried about how the EU will handle the validation of an ID card issued by an EU Member State, how the security of this ID card will be guaranteed, and how a person's physical identity will be linked to their digital ID card. Onfido also wonders how lost or compromised devices will be dealt with and whether the EU will allow third parties to access a digital identity with the user's permission. Onfido suggests increasing security by making it mandatory for governments to include a biometric authentication mechanism in their wallets.

The Foundation for Internet Domain Registration in the Netherlands (SIDN) welcomes the Commission's proposal and highlights that any solutions should allow end users to manage and control their digital identity, associated attributes and credentials in a free and open manner. SIDN is nevertheless worried that the proposal does not prevent the development of identification means that are not freely accessible to qualified and non-qualified trust service providers and does not prevent ID wallets from having secondary commercial purposes.

Some stakeholders have also warned about incorporating unique identifiers in digital IDs. For example, a representative of the digital rights umbrella group European Digital Rights said that such devices would be illegal or unconstitutional in certain countries.

Browser makers have expressed serious misgivings about supporting and displaying additional trust certificates such as QWACs. According to some analysts, much 'highly nuanced' web infrastructure work would need to be done by third parties for them to be able to interoperate with this EU requirement. Mozilla Corporation, for instance, is worried that the requirement would inadvertently expose EU citizens and residents to untenable security risks and roll back years of progress in security on the web.

After the Parliament and the Council reached a provisional agreement on this file, in November 2023 Mozilla Corporation repeated the concern raised above, arguing that the amended eIDAS

Regulation radically expands 'the capability of EU governments to surveil their citizens'. In the same article it also claimed that EU Member States will be able 'to designate cryptographic keys for distribution in web browsers and browsers are forbidden from revoking trust in these keys without government permission'.

Hundreds of scientists, researchers and NGOs around the world have signed an open letter expressing similar concerns. The signatories ask the co-legislators to reconsider the text to make it clear that Article 45 will not interfere with trust decisions around the cryptographic keys and certificates used to secure web traffic. The signatories also believe that the provisionally agreed text would still enable governments and service providers to 'link together and gain full knowledge about the uses of credentials in the new European Digital Identity System'.

Several internet infrastructure and security companies have made similar comments in a joint statement published in November 2023. They also criticise Article 45 for obliging browsers to recognise new website authentication certificates and claim that the formulation of the article is imprecise.

European Signature Dialog (ESD)[5] disagrees with this criticism, arguing that the amended eIDAS Regulation (in particular Article 45) would increase internet security, transparency and trust. ESD supports the provisional agreement and reminds that QWACs are not a new form of website authentication certificates. The updated eIDAS Regulation simply asks web browsers to display clearly the identity information of website owners. ESD also reminds that providers issuing QWACs are subject to rigorous security checks and audits.

Government IT security company Bundesdruckerei believes also that QWACs would help to increase trust in the digital space and avoid that big tech companies outside the EU abuse their dominant position. According to Bundesdruckerei, websites with verified identities help to protect consumers and data.

German digital association Bitkom also supports the provisional agreement, in particular the formulation of Article 45. Bitkom criticises the current system allowing browsers to impose their own rules and is in favour of the proposed changes that would make it possible to apply European rules to European web traffic. Bitkom reminds that under the agreed text, browsers are still allowed to take action in the event of security concerns and to suspend QWACs.

Legislative process

Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy (ITRE); the rapporteur is Romana Jerković (S&D, Croatia). The committees for opinion are the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Legal Affairs (JURI) and the Committee on Civil Liberties Justice and Home Affairs (LIBE).

The rapporteur published her draft report on 31 May 2022, in which she proposed a number of changes as regards the structure, cybersecurity and privacy of the European digital identity wallet. She also proposed introducing a new chapter on governance to facilitate cross-border coordination and establishing a harmonised framework for digital identity.

The other committees involved in the legislative procedure in Parliament also flagged various issues relating to the wallet. For example, JURI's opinion, adopted in November 2022, highlighted how important it is to ensure the wallet's high level of security, including the encryption of content. IMCO's opinion, adopted in September 2022, focused, among other things, on improving consumer choice through the possibility of keeping track of transactions, blocking access to the wallet in the event of a security breach, enabling the use of different devices, and offering the possibility to contact the wallet's issuer easily.

The ITRE committee adopted its position on 9 February 2023, which was then backed in plenary on 16 March (with 418 votes in favour, 103 votes against, and 24 abstentions) and confirmed as the Parliament's mandate for negotiations with the Council. The Parliament proposed a number of

changes in the structure of the European digital identity wallet. In particular, it insisted on expanding the use of the wallet, by enabling citizens not only to prove their identity and share documents but also to verify companies' and other citizens' identities and documents. It also emphasised that the wallet should remain voluntary, free of charge for individuals as well as businesses, and that users should be able to keep track of all transactions executed through the wallet. Parliament insisted that Member States issue the wallet 18 months (and not 12 months as proposed by the Commission) after the amended eIDAS Regulation's entry into force. Parliament also proposed amendments to reinforce both the cybersecurity and the privacy of the wallet, by asking explicitly that the wallet ensure cybersecurity and privacy by design. Parliament also suggested that a new chapter on governance would be added to facilitate cross-border coordination and the establishment of a harmonised framework for digital identity. Finally, Parliament modified the provisions on QWACs.

On 6 December 2022, the Council adopted its position (general approach) on the file. The Council proposed to develop further the concept of the wallet and its interplay with national electronic identification means. It also suggested to amend the text as regards the wallet's functioning, to ensure that the person claiming an identity is actually the holder. According to the Council text, Member States would have 24 months to provide the wallet, counting from the moment the implementing acts enter into force. Furthermore, the Council proposed amendments to align the text with other EU laws, such as the cybersecurity legislation. Finally, the Council considered that the wallet should be free of charge for individuals, while businesses may incur costs for authenticating with the wallet.

The European Parliament and Council negotiators reached a provisional agreement on the file on 8 November 2023. Below are the main points of the provisionally agreed text:

- Member States have to provide[6] citizens and businesses with a European digital identity wallet that allows users to digitally identify themselves, store and manage identity data and official documents (such as driving licences, university diplomas, medical prescriptions) in digital form in all EU countries. The wallet can also be used to digitally sign documents. The European digital identity wallets can be provided either by the Member State itself or by a private-sector provider.
- The wallet is voluntary and free of charge for individuals, while businesses may incur costs. It does not replace existing identification and authentication means but complements them.
- The wallet contains a dashboard of all transactions and offers the possibility to report alleged violations of data protection. Users can also request that their data be deleted.
- The wallet should ensure the highest level of data protection and implement advanced security features such as state-of-the-art encryption and storage methods.
- Whenever there is no legal requirement for users to have a legal identity for authentication, they will be able to use freely chosen pseudonyms.
- Very large online platforms[7] will have to accept the European digital identity wallet when users wish to log in on them.
- Member States have to disclose the source code of the user application software components of the wallet to enable members of the public to understand its operation and to be able to audit and review its code. The disclosure of the source code may be limited for public security purposes.
- The Commission has to establish a European Digital Identity Cooperation Group[8] to support and facilitate cooperation among EU Member States.
- Web browsers are required to recognise QWACs, so that users can verify the identity of persons or legal entities behind a website. This identity data has to be displayed in a user-friendly manner. In case of substantiated security concerns, web browsers are still allowed to take precautionary measures related to these certificates.

The Committee of Permanent Representatives of EU Member States (Coreper) endorsed the agreement on 6 December 2023 and the ITRE committee then did likewise the following day (35 votes in favour, 13 against, and six abstentions).

The text now needs to be formally adopted by the Parliament[9] and the Council before it can be published in the Official Journal of the EU and enter into force.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS

Negreiro M., Path to the digital decade programme, EPRS, European Parliament, February 2023.

Negreiro M., The EU digital decade: A new set of digital targets for 2030, EPRS, European Parliament, August 2021.

Niestadt M., Electronic signatures, EPRS, European Parliament, December 2022.

Niestadt M., Qualified certificates for website authentication, EPRS, European Parliament, January 2023.

Tuominen M. with Festor S., Establishing a framework for a European digital identity: Initial appraisal of a European Commission impact assessment, EPRS, European Parliament, 2021.

OTHER SOURCES

European Digital Identity framework, Legislative Observatory (OEIL), European Parliament.

ENDNOTES

[1] In the context of the eIDAS Regulation, attributes refer to elements of personal information and data items from the individuals' identity criteria, such as nationality, sex, age, place of birth, etc.

[2] Later on, the digital compass targets regarding the digital ID were changed: 100 % of citizens should have access to a digital ID.

[3] See Article 5c:'Personal data shall be … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")'.

[4] This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'European Parliament supporting analysis'.

[5] Platform of major European electronic signature providers. ESD connects also qualified trust service providers (QTSPs) across Europe.

[6] Within 24 months after the entry into force of the implementing acts.

[7] As defined in the Digital Services Act.

[8] Composed of representatives of Member States and the Commission.

[9] The vote in the Parliament is currently planned for 26 February 2024.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Fourth edition. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.