cerre Centre on Regulation in Europe

eIDAS 2.0: DIGITAL IDENTITY SERVICES IN THE PLATFORM ECONOMY

ISSUE PAPER

October 2022

Christoph Busch

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Vodafone, Microsoft, Comreg. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHOR

Christoph Busch is Professor of Law and Director of the European Legal Studies Institute at the University of Osnabrück, Germany. He is a Fellow and Council Member of the European Law Institute (ELI) and an Affiliated Fellow at the Information Society Project at Yale University. His research focuses on consumer law, platform governance and algorithmic regulation.

EXECUTIVE SUMMARY

In recent years, digital identity services have seen an increasing demand by businesses and users across various sectors, including healthcare, education, banking, e-commerce and mobility. The COVID-19 pandemic has further accelerated the digital transition and increased the need for digital identity solutions. As a result, the market for digital identity solutions has become a new major battleground in the digital economy. Key actors and competitors include banks, mobile network operators, and digital platforms offering single sign-on services. With its proposal for a revision of the eIDAS Regulation, published in June 2021, the European Commission aims to establish a new regulatory framework ("eIDAS 2.0") for digital identity solutions that meet the new market demands and gives citizens more control over their personal data. In addition, the Digital Markets Act (DMA) seeks to prevent platform envelopment and gatekeeping strategies regarding digital identity services and keep that market open. Against this background, this CERRE issue paper scrutinises the changing regulatory framework for digital identity solutions in the platform economy. It identifies key regulatory issues and makes policy recommendations for an innovative and competitive identity ecosystem that may benefit all players.

Key messages

- For the acceptance of the new European Digital Identity Wallet (EDIW), ensuring a high level of cybersecurity and privacy is of critical importance. Instead of introducing a persistent and unique identifier for all European citizens, a more privacy-friendly alternative seems preferable, an identifier that is unique per service and thus, does not allow tracking of users across different services, for instance.
- The regulatory framework for identity solutions should facilitate competition between different wallet apps, each meeting the relevant technical and legal requirements. In order to avoid lock-in effects and the creation of proprietary wallet ecosystems, users should be free to switch between different wallet providers and the technical solutions should allow for interoperability.
- For the effective enforcement of the new regulatory framework, an update of the existing rules on regulatory oversight and governance of digital identity services is necessary. In particular, the creation of a European Digital Identity Board (EDIB), consisting of national authorities and the Commission, could help to ensure the consistent application of the revised eIDAS Regulation and facilitate the exchange of best practices. It is important, however, that the purpose and governance of an EDIB are made very clear in order to avoid inconsistencies and overlaps with existing bodies at the European level.
- In the near future, it may be necessary to further expand the scope of the European digital identity framework. In particular, in the Internet of Things (IoT), an 'identity of things' could be necessary to facilitate autonomous interactions between connected objects. Furthermore, shared virtual worlds such as the Metaverse could create a need for new digital identity solutions, for distinguishing avatars representing humans and avatar bots, for example. To be future-proof, the technical architecture and the common standards that are currently being developed for the new eIDAS framework should consider these developments.

1. INTRODUCTION

Digital identities facilitate activity across platforms and services, making them the key to the digital world. Access to public and private services, including healthcare, banking, education, and mobility require secure and user-friendly identification solutions. The European legislator recognised this early on and created a legal framework for digital identities and trust services in the EU with Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).[1]

However, since the eIDAS Regulation came into force, the market for identity services has undergone fundamental changes. As the number of identity-sensitive and personalised services increases, secure online identification and the provision of trustworthy attributes and credentials are becoming more important than ever.[2] In the expanding market for digital identity solutions, providers of digital platforms "act as de facto digital identity gatekeepers and offer BYOI (bring your own identity) solutions that allow their users to authenticate on third-party websites and services by using their user profiles" (for example Login with Facebook, Login with Google).[3] In doing so, digital platforms are competing with banks, telecoms, and other providers of verified identities which seek to enable seamless traffic across digital services.

Over the past few years, the market for digital identity solutions has become a new major battleground in the digital economy. At this point, it is not yet clear whether a dominant provider will emerge in the future and who it could be. From an economic perspective, there are significant network and ecosystem effects in providing identity solutions that operate across multiple services (single sign-on). Therefore, it is likely that a dominant provider may emerge unless there is some mandated interoperability. In addition to these economic considerations, identity solutions raise important privacy issues[4] and, as the European Commission underlines in its evaluation report on the eIDAS Regulation, the "ability to identify digitally will become an important factor of social inclusion and the provision of digital identity is a strategic asset".[5]

In order to meet the changing demand for digital identity solutions in the EU, in June 2021 the Commission published a proposal for a revision of the eIDAS Regulation.[6] The proposal, which is commonly referred to as "eIDAS 2.0", introduces a European Digital Identity Wallet (EDIW). In doing

[1] Regulation (EU) 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 [2014], OJ L 257, hereinafter: Regulation (EU) 910/2014.

[2] European Commission, 'Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)', COM(2021) 290 final, [2], hereinafter: Report on the evaluation of the eIDAS Regulation, COM/2021/ 290.

[3] Ibid.

[4] EDPS, 'Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity', https://edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf, hereinafter: Formal comments on the eIDAS Proposal

[5] European Commission, 'Report on the evaluation of the eIDAS Regulation', COM(2021) 290, 2.

[6] Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity [2021] COM/2021/281 final, hereinafter: eIDAS Proposal.

so, it seeks to achieve a shift from the mutual recognition of national eIDs to a system that allows users to exchange electronic attestations of attributes authenticated by (qualified) trust service providers and gives users more control over their personal data. The new eIDAS framework is complemented by the Digital Markets Act (DMA) which seeks to prevent platform envelopment strategies regarding digital identity services and keep the market for identification services open.

Against this background, this issue paper scrutinises the changing regulatory framework for digital identity solutions in the European Union and seeks to develop policy recommendations. As such, it aims to contribute to the current debate about the governance of digital identity services in the platform economy. The remainder of this issue paper is organised as follows: section 2 provides a concise overview of the market for digital identity services in the EU. It briefly outlines key concepts, market trends, and identifies the main market actors. Section 3 outlines the regulatory trajectory at EU level from the 2014 eIDAS Regulation to the 2021 revision proposal. It also addresses the potential impact of the DMA on the market for digital identity services. Section 4 identifies several key regulatory issues that are crucial for the future regulatory framework for digital identity services in Europe, and develops recommendations for the revision of the EU digital identity framework.

2. THE MARKET FOR DIGITAL IDENTITY SERVICES

2.1 Digital identity and attributes

The eIDAS Regulation does not provide a formal definition of 'digital identity'. Instead, it refers to "electronic identification"[7] as a process and to "electronic identification means" as "a material and/or immaterial unit containing person identification data and which is used for authentication for an online service".[8] Similarly, the DMA defines "identification services" as " a type of service provided together with or in support of core platform services that enables any type of verification of the identity of end users or business users, regardless of the technology used".[9] For the purposes of this issue paper, **a digital identity can be defined as a digital representation of a natural or a legal person which allows the identity holder to prove who they are during online or offline interactions and transactions.**[10] In policy debates, the term digital identity often covers a wide range of identity solutions including national electronic identification documents (eIDs), online banking accounts or social media accounts. Irrespective of the different types of identity solutions, in all scenarios there are at least three parties involved: the issuer (or identity provider), the user (or identity holder) and the relying party (who consumes the identity provided by the issuer).

Besides digital identities as such, the provision and reliance on specific attributes related to those identities have become more and more important for digital transactions.[11] With a digital identity, such as a digital ID card, people can only prove who they are, but not what qualifications or credentials they have. However, such attributes are often necessary to access a digital service. Therefore, other attributes such as medical certificates, professional qualifications, driving licences, or e-tickets that are linked to a digital identity and authenticated by a (qualified) trust service provider have become essential elements of digital identity systems.

2.2 Growing demand for digital identity services

In recent years, digital identity services have seen an increase in demand by businesses and users as a result of the digitalisation of all areas of societal and economic activities. The Covid-19 pandemic has further accelerated the digital transition and increased the need for digital identity solutions. The example of the digital Covid certificates shows how much electronic identification solutions have become part of our everyday lives. Other examples of online activities that require secure digital identities include remotely opening a bank account, authenticating online payments for e-commerce transactions, renting a car, paying taxes, or enrolling in a university. For all of these use cases, citizens

[7] Regulation (EU) 910/2014, art 3(1).
[8] Regulation (EU) 910/2014, art 3(2).
[9] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265, art 2(19), hereinafter: Digital Markets Act.
[10] European Commission, 'Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity', SWD(2021) 124 final, pt 1, para 6, hereinafter: SWD (2021) 124 final.
[11] Ibid.

and businesses expect a high level of security and privacy, seamless customer journeys, and a convenient and intuitive user experience.

With the increasing number of identity-sensitive and personalised services and the diversification of use cases for electronic identification, demand has shifted from digital identities as such towards the exchange of individual attributes related to those identities (e.g., verification of age, professional qualifications, driving licences and other credentials). As the European Commission underlines in the explanatory memorandum accompanying the proposal for the revised eIDAS Regulation ("eIDAS 2.0") "this has triggered a paradigm shift, moving towards advanced and convenient solutions that are able to integrate different verifiable data and certificates of the user. Users expect a self-determined environment where a variety of different credentials and attributes can be carried and shared such as for example your national eID, professional certificates, public transport passes or, in certain cases, even digital concert tickets. These are so-called self-sovereign app-based wallets managed through the mobile device of the user allowing for a secure and easy access to different services, both public and private, under his or her full control".[12]

2.3 Types and providers of digital identity services

Historically, providing a secure identity to citizens has been the prerogative of governments. Today, government-issued identification documents (e.g., ID cards) are still an important means of identification for offline transactions. Digital identity services, however, are no longer solely provided by governments, but can also involve a broad range of private sector actors.[13] The market for digital identity services in the EU is diverse and fragmented. While some Member States (e.g., Belgium) have government-led public digital identity ecosystems, other Member States have bank-led private digital identity ecosystems (e.g., Nordic countries). Furthermore, across the EU, digital identity solutions provided by governments, such as national eIDs, coexist with a broad variety of private sector digital identity services offered by banks, telecoms, and social media platforms.[14]

In line with the eIDAS Regulation, several Member States have notified eID schemes to the Commission.[15] These **government-issued eIDs** provide a high level of trust as they are based on strict rules and processes for identity proofing and are mostly used for accessing public services. For many online services, **single sign-on services** offered by digital platform providers (e.g., Google Sign-In, Facebook Login) have gained popularity. These services, which are commonly referred to as 'social logins', allow users to access a broad range of applications and websites by connecting through a platform account rather than using a separate identity and password on each website. While social logins provide convenient solutions for many online services, they cannot be used for services that

[12] eIDAS Proposal, 48.
[13] Deloitte, 'The user experience of eIDAS-based eID' (2018), 18
[14] The following overview is based on European Commission, SWD(2021) 124 final, pt 1, 7-8.
[15] European Commission, 'Overview of pre-notified and notified eID schemes under eIDAS', (2 January 2019) https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

require a higher level of assurance in the identity of the person (e.g., banking).[16] Moreover, it is problematic both in terms of competition and from a data protection point of view that social login providers are able to track user activity across multiple unaffiliated websites and apps.[17]

In some Member States, especially in the Nordic countries, digital identity solutions offered by **banks** have gained considerable popularity. In Sweden, for example, the electronic identification service BankID has 8 million users.[18] In contrast, in other Member States digital identity services offered by banks remain closed to external services. **Mobile network operators** are also important providers of digital identity services. As many countries mandate the registration of SIM cards, mobile network operators have to verify the identities of their customers before activating their services and granting them access to the network. As a consequence, they can provide a higher level of assurance in the identity of the person than other identity services.

[16] More recently, digital platforms seek to provide digital identity solutions with higher levels of assurance in connection with payment services (e.g. Apple Pay, Google Pay), cf. European Commission, SWD(2021) 124 final, pt 1, p 8.
[17] See, e.g. Jan Krämer, Daniel Schnurr and Sally Broughton Micova, 'The Role of Data for Digital Markets Contestability' (2020), CERRE Report, s 4.1.3.
[18] BankID, 'BankID i siffror' https://www.bankid.com/om-oss/statistik

3. TOWARDS A NEW REGULATORY FRAMEWORK FOR DIGITAL IDENTITY SERVICES

This section briefly outlines the **regulatory trajectory at EU level** from the 2014 eIDAS Regulation ("eIDAS 1.0") to the 2021 Regulation revision proposal ("eIDAS 2.0"). It also addresses the potential impact of the DMA on the digital identity services market.

3.1 eIDAS 1.0 Regulation

With the eIDAS Regulation, in 2014 the European Union created a regulatory framework for trusted electronic identification of natural and legal persons, and trust services (e.g., digital signatures). Under the eIDAS framework, all Member States committed to mutually recognising government-issued eIDs. For this purpose, **the eIDAS Regulation created a notification scheme and encouraged Member States to notify national eIDs to the Commission.** EU citizens should be enabled to use their national identities to access public services in other EU countries or sign a document with a secure electronic signature. It is important to note that the eIDAS Regulation did not introduce a harmonised European digital identity, but rather aimed at ensuring mutual recognition and interoperability between existing digital identity schemes at national level. Moreover, the eIDAS Regulation did not oblige Member States to create national eID schemes and to notify them to the Commission.

The Impact Assessment of the eIDAS Regulation has shown that the existing regulatory framework has only partially achieved its objectives.[19] In particular, the eIDAS framework focuses on the secure cross-border access to public services, which are mainly relevant to a small proportion of the EU population. Moreover, the Regulation only offers limited possibilities for providers of private services to connect to the eIDAS system. A further weakness of the existing eIDAS framework is that it does not cover the provision of electronic attributes, such as medical certificates, driving licences or professional qualifications.[20] In addition, it does not allow users to limit the sharing of identity data to what is strictly necessary for the provision of a service. The Impact Assessment also noted that only 14 Member States had notified eIDs and only 59% of EU citizens had access to cross-border digital identity solutions in accordance with the eIDAS Regulation.[21] In addition, usage rates and the number of available public services offered vary considerably among Member States. While the bank-led systems in the Nordic region reach almost the entire population and offer access to a large number of public and private services, other Member States have only a low uptake of digital identity schemes or have no digital identity solution at all. In summary, the eIDAS framework in its current form falls short of addressing new market demands that have risen since it entered into force in 2014.

[19] SWD(2021) 124 final, pt 1, para 4 et seq.
[20] Part 1, SWD(2021) 124 final, pt 1, para 2-3, 10-12.
[21] Part 1, SWD(2021) 124 final, pt 1, 4.

3.2 eIDAS 2.0 Regulation

In order to remedy the weaknesses of eIDAS 1.0, in June 2021 the European Commission published a **proposal for a revision of the eIDAS Regulation**.[22] The proposal seeks to address the shortcomings of the existing regulatory framework and extend its benefits to a broader range of use cases in the private sector. While the existing eIDAS framework relied on the voluntary cooperation of Member States, the new proposal requires each Member State to offer and notify a digital identity solution. Under the new Regulation, they will be obliged to offer the **European Digital Identity Wallet** (EDIW).[23] The EDIW is essentially a software application that allows for the online and offline identification of citizens and residents based on national digital identities. In addition to storing their eIDs, users shall be able to add other electronic attributes and credentials to their wallets such as university degrees, diplomas, student IDs or a driver's license.

While using the EDIW shall remain voluntary for EU citizens, public sector bodies and private parties that are required by national law or EU law to use strong user authentication for online identification are obliged to accept the wallet as a means of digital identification.[24] As a consequence, **acceptance of the EDIW will be mandatory across many sectors** (e.g., banking, energy, healthcare). More importantly, the proposal extends the mandatory acceptance of the EDIW to very large online platforms (VLOPs),[25] which reach a number of average monthly active recipients of the service in the Union equal to or higher than 45 million.[26] Where VLOPs, such as Amazon, Facebook, or Google, require users to authenticate to access online services, they will be required to accept the EDIW as a means to log into their services if their users ask for it.[27] Furthermore, the Commission can mandate smaller providers of digital services to accept the wallet via a delegated act based on an assessment of usage patterns of the EDIW.[28]

In parallel with the revision of the regulatory framework, the Commission also seeks to create a **common technical architecture and common standards** for digital identity solutions to prevent further fragmentation resulting from divergent national identity solutions. For this purpose, the proposal for a revision of the eIDAS Regulation is accompanied by a Recommendation[29] which sets out a process for the development of a **Toolbox** that defines the technical requirements for the EDIW. The Toolbox is currently being developed in collaboration with the Member States by an eIDAS expert group.[30] A first summary description of the eIDAS expert group's understanding of the EDIW concept

[22] eIDAS Proposal
[23] eIDAS Proposal, art 6a
[24] eIDAS Proposal, art 12b(1), art 12b(2)
[25] eIDAS Proposal, art. 12b(3)
[26] See Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2020] COM/2020/825 final, art 25(1), hereinafter: Digital Services Act
[27] eIDAS Proposal, art 6a(3)
[28] eIDAS Proposal, art 12b(5)
[29] European Commission, Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.
[30] For more information about the eIDAS Expert Group see: European Commission, 'Register of Commission Expert Group and Other Similar Entities, eIDAS Expert Group (E03032)' https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3032

was published in February 2022.[31] The document outlines, among other things, the roles of the different actors in the digital identity system and several potential use cases for the wallet.[32]

In May 2022, the **ITRE Committee** of the European Parliament published its draft report on the proposal for the revised eIDAS Regulation[33] which contains a large number of amendments. The most relevant of those will be discussed in Part 4 of this issue paper. In addition, the **Opinion of the European Parliament's IMCO Committee**, which was adopted in September 2022, underlines the need to ensure consumer choice and appropriate safeguards in case of a security breach.[34]

3.3 Digital Markets Act

As discussed above, single sign-on services offered by digital platforms have become popular among Internet users in recent years. The increasing adoption of these services allows digital conglomerate platforms such as Google and Facebook to gather data from third-party websites which further increases their ability to provide targeted advertising, develop personalised services and identify attractive adjacent markets.[35] In this regard, single sign-on services may further strengthen the market power of digital gatekeepers and allow them to expand into neighbouring markets.[36]

Considering the importance of network effects and the financial strength of digital gatekeepers, they could soon become dominant players in the market for identity solutions. Against this background, the DMA prohibits designated gatekeepers from imposing any restrictions on business users regarding the use of competing identification services.[37] Article 5(7) DMA stipulates that "the gatekeeper shall not require end users to use, or business users to use, to offer, or to interoperate with, an identification service […] of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services". This prohibition seeks to mitigate competition concerns that may arise from the bundling of the gatekeeper's core platform services with the gatekeeper's own identification solutions. It aims to protect the freedom of business users and end users to choose alternative services to the ones of the gatekeeper.[38] From an economic perspective, the provision seeks to prevent platform envelopment strategies and keep the market for identification services open. In other words, gatekeepers shall not extend their market power into the adjacent

[31] European Commission, 'European Digital Identity Architecture and Reference Framework, Outline' (22 February 2022) https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

[32] The use cases include the following five topics: Secure and trusted identification to access online services, mobility and digital driving licence, health, education, and digital finance.

[33] European Parliament, Committee on Industry, Research, and Energy, 'Draft Report on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity', 2021/0136(COD), 31 May 2022, hereinafter: ITRE Report.

[34] European Parliament, Committee on the Internal Market and Consumer Protection, 'Opinion on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 14 September 2022', 2021/0136(COD), hereinafter: IMCO Opinion.

[35] European Commission, 'Digital Markets Act: Impact Assessment Support Study, Executive Summary and Synthesis Report' (2020), 16

[36] See also Jan Krämer, Daniel Schnurr and Sally Broughton Micova, 'The Role of Data for Digital Markets Contestability' (2020) CERRE Report, s 4.1.3

[37] Digital Markets Act, art. 2(19) defines identification services as "a type of service provided together with or in support of core platform services that enables any type of verification of the identity of end users or business users, regardless of the technology used".

[38] Digital Markets Act, Recital 43.

market for digital identification solutions requiring the business user to use the gatekeeper's own services.[39]

From the wording of Art. 5(7) DMA it is not entirely clear whether the provision only applies to single sign-on services that the designated gatekeeper provides for third-party websites and applications or whether the provision also requires the gatekeeper to accept alternative identification solutions for its own services. If the main purpose of the provision is to keep the market for identity services open, a narrow interpretation of Art. 5(7) DMA seems favourable. As a consequence, for example, a gatekeeper may not require app developers to use its own single sign-on service (e.g., Sign in with Apple, Google Sign-In) to be eligible for access to the app store. In contrast, according to this narrow interpretation, the DMA does not oblige the gatekeeper to accept third-party identification solutions for its own core platform services (e.g., for signing into the app store). However, as discussed above, the proposal for a revised eIDAS Regulation mandates very large online platforms under Art. 25 of the Digital Services Act (DSA) to accept the EDIW if their users ask for it.

[39] Giorgio Monti, 'The Digital Markets Act – Institutional Design and Suggestions for Improvement' (2021) TILEC Discussion Paper 2021-004, 3 https://ssrn.com/abstract=3797730

4. REGULATORY ISSUES AND RECOMMENDATIONS

This section identifies several key regulatory issues that are crucial for the future regulatory framework for digital identity services in Europe and develops recommendations for the revision of the EU digital identity framework.

4.1 Market structure for digital identity services

4.1.1 Competition between wallet providers

The proposal for a revised eIDAS Regulation envisages that Member States must issue one or several EDIWs within 12 months after the Regulation enters into force.[40] For this purpose, the eIDAS Regulation gives Member States the choice between several options.[41] In the first option, the Member State itself issues a wallet for its citizens and businesses or commissions a single provider to develop the wallet app under a government mandate. A second option is for the Member State to define the regulatory and security framework and allow several private-sector wallet apps to be developed and recognised by the Member State. Among these two options, **competition between different wallet apps, each meeting the relevant technical and legal requirements, seems to be preferable for promoting innovation and freedom of choice** as this approach allows citizens to freely decide which wallet they want to use. In particular, this approach could lead to a fruitful combination of government-issued eIDs with private sector innovations for user-friendly identity solutions. This approach requires a technical solution that enables interoperability with other platforms.

4.1.2 Switching and multi-homing

In order to avoid lock-in effects and the creation of proprietary wallet ecosystems, users should be free to switch between different wallet providers.[42] Moreover, non-discriminatory access to key elements of hardware and software should be ensured. The Commission's proposal for a revised eIDAS Regulation does not expressly stipulate a right to 'identity portability'. In contrast, the draft report of the European Parliament's ITRE Committee suggests adding a Recital to the Regulation which would underline that "the issuers of the European Digital Identity Wallets should at the request of the user of the Wallet, provide for effective portability of data, including provisions of continuous and real-time access to services, and not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different European Digital Identity Wallets".[43]

The requirement of "continuous and real-time access" would go beyond a mere portability right that allows the transfer of the stored identity data to another wallet when a user decides to switch from one wallet provider to another. **Seemingly, the draft ITRE report seeks to enable effective multi-**

[40] eIDAS Proposal, art 6a(1)
[41] eIDAS Proposal, art 6a(2)
[42] Cf. Joshua Gans, 'Enhancing Competition with Data and Identity Portability' (2010) Brookings Institution, Policy Proposal 2018-10 https://www.brookings.edu/wpcontent/uploads/2018/06/ES_THP_20180611_Gans.pdf
[43] ITRE Report, Amendment 18, 18

homing between different EDIWs. From the perspective of users, it might also be desirable to use different identity solutions in parallel for different social contexts, one wallet for healthcare services and another wallet in the context of education, for instance. The technical solutions chosen for the EDIW should make this possible.

In addition, another proposed amendment in the ITRE Report points in a similar direction. Thus, the report suggests that the EDIW should "provide a mechanism for the synchronization of European Digital Identity Wallets belonging to the same user, upon his or her request".[44] However, from a technical perspective, enabling real-time synchronisation of different wallets for the purpose of multi-homing could pose significant challenges compared to a mere portability requirement. Therefore, **it has to be carefully examined whether the advantages of multi-homing justify the technical effort and possible risks in terms of security and privacy.**

4.2 Cybersecurity and privacy

Acceptance and take-up of the EDIW depends critically on whether the wallet app offers a user-friendly onboarding process, an intuitive user experience, and access to a broad range of use cases across different sectors.[45] Another critical factor will be whether citizens will have trust in the new wallet app. For this to happen the wallet must offer a high level of cybersecurity and privacy. In this respect, the fate of the digital driver's license introduced in Germany in September 2021 can serve as a cautionary tale. Less than a week after its launch,[46] the release of the German digital driver's license and the ID Wallet app was halted due to massive technical problems.[47] The ID Wallet app did not work for numerous users due to an inadequate IT infrastructure and generated multiple error messages. In addition, there were reports about serious security concerns.[48] Against this background, aspects of cybersecurity and privacy should be given the highest priority when EDWI is introduced.

4.2.1 Persistent and unique identifier

In this context, one of the most controversial aspects of the Commission's eIDAS proposal is the envisaged introduction of a persistent and unique identifier for all European citizens and residents.[49] This persistent and unique identifier would be shared by the wallet app with private and public third parties. **In some Member States, including Portugal[50] and Germany, the introduction of a uniform personal identification number would probably be considered unconstitutional.** According to the

[44] ITRE Report, Amendment 59, 38

[45] Cf. Lucas Wiewiorra, Andrea Liebe, Serpil Tas, 'Die wettbewerbliche Bedeutung von Single-Sign-On- bzw. Login-Diensten und ihre Relevanz für datenbasierte Geschäftsmodelle sowie den Datenschutz' (2020) WIK Discussion paper No. 462, 26 (arguing that users of single sign-on services seem to put their security concerns aside for a fast and simple registration procedure).

[46] Zeit.de, 'Autofahrer können sich ab sofort digitalen Führerschein per App holen' (24 September 2021) https://www.zeit.de/mobilitaet/2021-09/digitaler-fuehrerschein-verkehrsministerium-app-smartphone-mietwagen-carsharing

[47] Zeit.de, 'Digitale Führerschein-App defekt' (30 September 2021) https://www.zeit.de/mobilitaet/2021-09/verkehrsministerium-digitaler-fuehrerschein-app-defekt-andreas-scheuer

[48] Corinna Budras, 'Warum sich die Einführung des digitalen Führerscheins verzögert' *Frankfurter Allgemeine* (29 September 2021) https://www.faz.net/aktuell/wirtschaft/digitec/einfuehrung-des-digitalen-fuehrerscheins-verzoegert-sich-17561439.html

[49] eIDAS Proposal, art 11a

[50] See Constitution of the Portuguese Republic, art 35(5)

German Federal Constitutional Court, a general personal identification number for all public services that makes it possible to "register and catalogue the individual citizen in his or her entire personality" is unconstitutional.[51] Moreover, if users of the wallet are induced to share the unique and persistent identifier with private parties this could open the door to an unprecedented level of tracking and profiling of consumers. This could also create an incentive for "overidentification", i.e. the excessive use of the EDIW for online activities for the purpose of user profiling.

Against this background, the European Data Protection Supervisor (EDPS) in its formal comments on the eIDAS proposal raised concerns about the planned introduction of a persistent and unique identifier.[52] On the one hand, the EDPS acknowledges that the identifier could enhance the trust and integrity of the EDIW by reducing the risk of abuse or ambiguity errors. On the other hand, he notes that the identifier could create additional privacy risks and recommends exploring alternative means to enhance the security of matching. In this regard, it is a good sign that according to recent news reports the European Commission is moving away from the idea of a persistent and unique identifier.[53] **A more privacy-friendly alternative could be a model which uses an identifier that is "unique per service" and thus does not allow tracking of users across different services.** Such a model of sector-specific personal identifiers (ssPIN) is currently used in Austria, for instance.[54]

4.2.2 Privacy by design

In addition to the privacy concerns related to the persistent and unique identifier, it is important that the future European digital identity framework contains strict privacy safeguards and ensures that citizens have full control of their personal data when using the wallet. For this purpose, **the EDIW shall follow the privacy by design principle.** For example, as requested in the draft report of the ITRE Committee, tracking the use of the wallet or specific attributes must be technologically impossible for issuers of the EDIW.[55] Similarly, for issuers of the electronic attestation of attributes, it must be technologically impossible to track the use of these attributes by wallet users.[56]

From a privacy perspective, it is also important that the design of the EDIW follows the principle of data minimisation. This means that the sharing of data between wallet holders and relying parties is limited only to the data necessary for the specific purpose. If, for example, the purpose is age verification (e.g., for gambling or purchasing alcoholic beverages), only the date of birth should be shared but no other personal information (e.g., name, address). Depending on the use case, it could even be sufficient to design the app in such a way that it merely indicates whether a person is older than 18 years without sharing the exact date of birth. **An even higher level of privacy protection could**

[51] Federal Constitutional Court [1983] Case 1 BvR 209, 269, 362, 420, 440, 484/83, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983, para 119
[52] EDPS, Formal comments on the eIDAS Proposal, 4
[53] Laura Kabelka, 'Commission says single identifier in eIDAS reform 'not necessary'' *Euractiv.com* (11 July 2022) https://www.euractiv.com/section/digital/news/commission-says-single-identifier-in-eidas-reform-not-necessary
[54] European Commission, 'eGovernment in Austria' (2018) https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Austria_2018_vFINAL.pdf
[55] See ITRE Report, Amendment 70, 42-43
[56] Ibid.

be achieved by using a zero-knowledge proof (ZKP) approach. As explained in the ITRE Report, ZKP "allows verification of a claim without revealing the data that proves it, based on cryptographic algorithms".[57] In the above example, age verification could be performed without submitting the date of birth. While the ZKP approach could considerably increase the protection of personal data in the context of electronic identification, **it has to be carefully assessed how reliable the ZKP technology is and for which use cases it could be considered.**

4.3 Governance of digital identity services

Considering the significant changes in the European digital identity system that the revision of the eIDAS Regulation will bring, it is somewhat surprising that the Commission's proposal leaves the provisions regarding regulatory oversight and governance provisions more or less unchanged. **Therefore, it is welcomed that the ITRE Committee in its draft report suggests adding an entirely new chapter on governance to the Regulation.[58]** According to the ITRE Report, each Member State shall establish one or more national authorities that shall be in charge of monitoring and enforcing the application of the revised eIDAS Regulation.[59] In particular, the competent authorities shall supervise the issuers of the EDIWs, relying parties and qualified trust service providers.[60] Considering the growing practical importance of digital credentials (e.g., professional qualifications, driver's licences), one can expect that there will be more oversight work for existing national authorities under eIDAS 2.0 regarding providers who authenticate the attestation of attributes.

Furthermore, the creation of a 'European Digital Identity Board' (EDIB), which has been suggested in the draft report of the ITRE Committee, could help to ensure the consistent application of the revised eIDAS Regulation and facilitate the exchange of best practices.[61] The EDIB, which shall be composed of the national competent authorities and the Commission, could also assist the Commission in the preparation of implementing and delegated acts.[62] It is worth notingthat the proposal to establish the EDIB has been modelled after similar bodies at EU level, such as the Body of the European Regulators for Electronic Communications (BEREC), the European Data Protection Board (EDPB) or the new European Board for Digital Services (EBDS), which will be introduced by the DSA.[63]

On the one hand, the creation of such bodies at the European level can certainly contribute to the consistent application of EU regulations. On the other hand, the multiplication of European "Boards" for specific regulatory topics increases the overall complexity of the governance architecture for digital markets and requires careful coordination between the different regulatory bodies to avoid overlaps and inconsistencies. It has to be decided whether privacy issues regarding the EDIW should be addressed by the EDPB or by the EDIB, for instance. **Therefore, if the proposal of the ITRE Committee**

[57] ITRE Report, Amendment 10, 12
[58] ITRE Report, Amendment 131, 73 et seq.
[59] ITRE Report, Amendment 131, art. 46a(1),73
[60] ITRE Report, Amendment 131, Art. 46b(1), 74
[61] ITRE Report, Amendment 131, Art. 46c, 77
[62] ITRE Report, Amendment 131, Art. 46c(5)(b), 77
[63] Digital Services Act, art 47

is taken up, the EDIB should become a member of the high-level group of European bodies created under Art. 40 DMA.

4.4 Expanding the digital identity framework

4.4.1 Corporate digital identities

Digital identities are not only an important digital tool for citizens. Businesses also need secure and trustworthy identity solutions. The eIDAS Regulation of 2014, which applies to natural persons and legal persons recognised this need for **corporate digital identities**. Similarly, several member states have introduced a legal framework for digital identities, especially for businesses. One recent example is the German pilot project for a 'digital corporate account' which is only applicable to public services.[64] The proposal for a revision of the eIDAS Regulation also extends the new digital identity framework to legal persons. Therefore, legal persons will also be able to use an identity wallet as identification means.[65]

So far, the policy debate about the revision of the eIDAS framework has mainly focused on the risks and benefits for citizens and consumers. However, **for the success of the new European digital identity framework, it is important that the implementation also considers the specific identification needs of businesses.** Irrespective of the revision of the eIDAS framework, financial institutions that are already experienced in Know Your Customer (KYC) processes could also play a leading role in the market for digital identity solutions for businesses. Similarly, the new Know Your Business Customer (KYBC) rules for third-party traders on online marketplaces introduced by the DSA could also serve as a basis for corporate digital identities that could be verified by platform operators.[66]

4.4.2 Digital identity in the Internet of Things and the Metaverse

In the near future, it may be necessary to even further expand the scope of the European digital identity framework. **In particular, in the Internet of Things, an 'identity of things' could be necessary to facilitate autonomous interactions between connected objects** (e.g., automated parking systems for connected vehicles). In this perspective, the draft report of the European Parliament's ITRE Committee rightly suggests that the implementing technologies and standards that are being developed for a European digital identity "could be extended to establish digital identities for connected objects in order to develop a trust layer for the development of Internet of Things".[67] Therefore, a possible extension of the digital identity framework to 'identity of things' should be taken into account when developing the technical architecture and common standards for the revision of the eIDAS framework. **Furthermore, shared virtual worlds such as the Metaverse could create a need**

[64] Marc Beise, 'Behördengänge werden digital' *Süddeutsche Zeitung* (1 June 2021) https://www.sueddeutsche.de/wirtschaft/unternehmenskonto-elster-neu-1.5308830
[65] eIDAS Proposal, art 6a(1)
[66] See Digital Services Act, art 24c
[67] ITRE Report, Amendment 3, 8

for new digital identity solutions.[68] For example, digital identities for avatars representing real humans could become necessary to distinguish them from avatar bots.

[68] Eileen Yu, 'Banks have opportunity to plug digital identity gap in metaverse' *ZDNet.com* (21 July 2022) https://www.zdnet.com/finance/banks-have-opportunity-to-plug-digital-identity-gap-in-metaverse

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
@CERRE_ThinkTank
Centre on Regulation in Europe (CERRE)
CERRE Think Tank