TOWARDS A EUROPEAN DIGITAL IDENTITY WALLET

Striking the right balance between regulation and market needs

21 June, 18:00-19:45 CET | European Parliament

Executive Summary

The evolution of the EU regulation on digital identity

The first EU act regulating digital identity, Directive 93/1999/EC, did not provide for any single set of rules for the so-called *'electronic identification'* (eID) instruments, thereby leading to creating a multitude of national systems with no certified interoperability between them. Also for this reason, **in 2014 the European Union issued the eIDAS Regulation** (electronic Identification, Authentication and trust Services), which is still the EU's reference provision on **electronic identification and trust services for electronic transactions.**

However, neither does this regulation harmonise national eIDs, and nor does it impose the creation of such instruments in countries where they do not exist, but rather establishes their mutual recognition and acceptance in cross-border transactions within the European Union. The eIDAS Regulation does not establish common technological standards but, instead, aims at binding diverse national eIDs in three levels of assurance (low, substantial and high) following certain minimum criteria and functional requirements. In addition to eID, the eIDAS regulation also provides a legal framework for trust services such as electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication certificates.

Since the adoption of the regulation, the focus on digital identities and authorisations has continued to grow in the EU, because of data protection and safety, privacy requirements (i.e., the GDPR regulation on privacy - EU 2016/679), as well as the higher technological and interconnectivity standards.

The idea that EU citizens are not in control of their digital identity has led the EU Commission to **recognise the gaining of full control of identity information, as well as limiting its use and abuse, as one of the pillars of the agenda for Europe's future and of the Next Generation EU plan**.

Therefore, on 3 June 2021, the European Commission published a **recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework** and a **proposal for a regulation amending Regulation (EU) n. 910/2014 as regards establishing a framework for a European Digital Identity**.

The recommendation underlines the importance of ensuring that online service providers can rely on digital identity solutions recognised across the Union, and encourages the strengthening of cooperation and the development of a **toolbox**, planned for September 2022, setting **common standards** and technical references as well as best practices and guidelines as a basis for the implementation of the European Digital Identity Framework. The proposal introduces a European Digital Identity Framework to offer users self-determined personal digital wallets that would allow for a secure and easy access to different services and **create a new qualified trust service for attestation of attributes concerning information related to identity**, such as addresses, age, gender, civil status, family composition, nationality, educational and professional qualifications and titles, licenses, other permits and payment data, that can be offered, shared and exchanged across borders. It also **prescribes each Member State to issue a European Digital Identity Wallet within 12 months after the entry into force of the regulation**, identifies permitted activities for users, defines **requirements of Digital Identity Wallets** and **gives the user full control** of the European Digital Identity Wallet.

The European Digital Identity Architecture and Reference Framework describes **the EUDI Wallet concept**, including objectives of the EUDI Wallet, roles of the ecosystem's actors, the wallet's functional and non-functional requirements and potential building blocks.

The spread of eID in Europe

Currently, **18 Member States have notified at least one eID scheme and 4 Member States have notified multiple schemes** for a **total of 22 eID schemes** registered so far. Although most of these schemes are legally guaranteed by national authorities, which are responsible for setting up and aligning the eIDs with national legislation**, the distribution and provision of the identities is often left to authorised market players**, thereby favouring market openness and competition.

At the same time, it is worth noting that **only 14% of key public service providers across all Member States allow cross-border authentication with an e-Identity system**, although it also reports a **rise in the number of cross-border authentications**. **Some countries** were already reporting to have approximately **covered the whole population** with the deployment of eIDs, such as Estonia (90% of total population) and the Scandinavian countries (all above 75% of adoption), while others were catching up (e.g. in Italy the *Spid ID* grew from 3.6% in 2018 to 47.4% in January 2022).

The spreading of eID service provided by private operators has proved to be quite consistent. According to the Final Report of the Study to support the impact assessment for revision of the eIDAS Regulation provided PwC and DLA Piper, **in 2020, there were 180 Qualified Trust Service Providers (QTSPs) in Europe.** The country with the highest number of QTSPs was **Spain (33),** followed by **France (22), Italy (21) and Germany (12). In terms of market value,** in 2018, the **total turnover** for the eID market was **€1.3 billion**, a value that is **likely to have increased considerably during the Covid years**. The projections of expected growth show **a rise to €3.8 billion by 2027**, representing a CAGR of 13.3% from 2018 to 2027.

The potential benefits of the European Digital Identity

Although the scheme still presents some limitations in terms of full adoption and interoperability, it offers a series of benefits which are now widely recognised not only in the public sector, but also among businesses and the general public. Here it is possible to see the **increased level of security** ensured by the common Levels of Assurance (LoA), included in eID schemes, improved **user experiences** (no longer the need to manage multiple digital identities on different platforms) and an **improving accessibility** to such services, **making the benefits of the digital revolution easily exploitable for the whole population.**

In addition, Eurostat data also shows that, **since the introduction of the eIDAS Regulation, European citizens have, on average, increased their eGov activities,** particularly those related to the provision and collection of bureaucracy-related forms, being also functional at enhancing administrative efficiency, reducing paperwork, speeding up processing, and reducing the risk of identity fraud.

Generally speaking, benefits arising from the spread of a digital identity are not only crucial for individual users of the digital environment, but also for **the business sector**, where **transactions are made safer** and **more efficient** thanks to the **interoperability** and the **common standards**. Indeed, by increasing formalisation in authentication procedures, which helps reduce fraud, protects rights, and increases transparency, **companies do not only cut security expenses**, a financial burden which has considerably increased in the Covid-19 transition period, **but also fixed costs.**

The debate on the eIDAS Regulation and Public Consultation

Even if the procedure is in the initial stage, some opinions have been expressed on the approach, aims and objectives pursued by the eIDAS Regulation. It has been noted that **the technical implementation of the act will take place through secondary legislation,** whereby it will be possible to **assess the compliance of the amended eIDAS with the GDPR only after the adoption of the implementing acts. Moreover, some technical risks stem from the creation of the centralised storage of identity data.**

The protection of personal data is essential for generating public confidence in the instrument and the proposing institutions. In this regard, some opinions have underlined the **need for the user to know exactly what data flows into the wallet and how it is used**.

A public hearing on the proposal was held at the ITRE committee last February. Considering the variety of functionalities to be aggregated, the **opportunity of proceeding in steps** has been noted, as well as the **preservation of the separation between European (qualified) electronic authentication services and national electronic identification schemes** for the time necessary for national authorities to establish these new schemes to **avoid private authentication services not being established while waiting** for the European Digital Identity Wallet to be agreed on by the 27 Member States. Here, some results of the Public Consultation also raise the **concern about the overlapping with existing solutions offered by private operators.** For example, this could be the case with the **lack of a clear distinction** between the ***identification procedures*** and the ***authentication procedures***, two apparently similar procedures, which nevertheless have certain specificities.

Concerns are also expressed for what regards the **possible effects on competition and innovation**, as well as for the **considerable weight that governments will hold in such a uniform scheme**. The possible market structure produced by the new regulation could envisage the **creation of 27 national identity schemes**, with **further market fragmentation** and major differences compared to the set-up in use today. In order to face the need for widely-spread and accessible digital e-Gov services, over recent years several national authorities have actually made use of **public-private-partnerships and of authorisation procedures involving private market players** in order to delegate to such entities the distribution and the releasing procedures of the required QTSs and eIDs.

On the contrary, the current version of the eIDAS Regulation could lead to a situation where selected players could become "*national champions*", also qualified as trust service providers. Hence, it would be very likely for them to count on an **undue competitive advantage** in the European market, being, at the same time, qualified as trust service providers plus running a national identification scheme. Evidence of such concerns is also provided by the Consultation, in which stakeholders suggest that the main corrective actions to be taken in the revision of the eIDAS involve an **obligation for Member States to make authentication available to the private sector** and allow for the **introduction of new private sector digital identity trust services** for identification, authentication and provision of attributes.

1. A Framework for a European Digital Identity. The European Commission proposal

Although there is no single definition, the concept of "*digital identity*" generally refers to all personal or personally related information that is digitally stored and accessible by the individual owning the information and, in some cases, by third parties as well. As most personal information is nowadays digitally stored, thus making it accessible independently of the physical location and time and usable for both public and private services, data and private information have become one of the key drivers of the digital society. At the European level, the attention on these developments, and on the consequences that they can have in a considerable number of activities in daily and professional life, has been increasing for more than 20 years. In response to the increasing use of specific systems for the creation of IT documentation in some Member States, i**n 1999 the European Community**, **adopted Directive 93/1999/EC**. For the first time in European history, homogeneous regulations were introduced for the use of **electronic signatures**, distinguishing three types of signatures (simple, advanced and qualified) and leaving wide margins of discretion to Member States as to their effective application. The **directive, however, did not provide for a single set of rules for the so-called *'electronic identification'* (eID) instruments, thereby leading to the creation of a multitude of national systems with no certified interoperability between them**, no precise rules for mutual recognition and no common protection for data in terms of privacy and for possible profitable purposes. In the following years, partly also thanks to the consolidation of the qualified electronic signature instrument, the need for greater uniformity was therefore revived. The underlying intention to create the 'EU Digital Single Market' was one of the major drivers of policy intervention aimed at regulating and harmonising a wider range of digital services. Within the Digital Market project, the electronic space was in fact intended as a digital ecosystem set on the fundamental principles of the EU relating to persons, businesses and goods, thereby placing major importance on data protection and service accessibility.

To address this situation, **in 2014, the European Union issued the eIDAS Regulation**[1] (electronic Identification, Authentication and trust Services[2]), which is still the EU's reference provision on **electronic identification and trust services for electronic transactions**.

[1]EU Regulation n. 910/2014 of the European Parliament and EU Council (23 July 2014). In force as from 1 July 2016.
[2]The five core trust services considered by the EU are: Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, and Qualified electronic registered delivery service.

The main purpose of the regulation is to achieve legal and technical interoperability among EU countries not only for electronic signatures, but also for electronic identification and authentication tools.

The regulation does not harmonise national eIDs, and nor does it impose the creation of such instruments in countries where they do not exist, **but rather establishes their mutual recognition and acceptance** in cross-border transactions within the European Union. This system is achieved through a **notification process**[3] which encourages the **creation of national digital identity systems that respect the uniform requirements and features set out in the regulation**. In compliance with the federated approach at the heart of the EU and the principle of technological neutrality, **the eIDAS Regulation does not establish common technological standards** but instead **aims at binding diverse national eIDs** in **three levels of assurance** (*low*, *substantial* and *high*[4]) following certain minimum criteria and functional requirements. In addition to eID, the eIDAS Regulation also **provides a legal framework for trust services** such as electronic signatures, electronic seals, time stamps, electronic delivery services and website authentication certificates. As for the eID, the regulation establishes the requirements to ensure that such trust services are provided and recognised across borders with the same legal effect in all Member States.

Since the adoption of the regulation, the focus on digital identities and authorisations has continued to grow in the EU. **Data protection** and **safety**, **privacy requirements** (i.e., the GDPR regulation on privacy - EU 2016/679), as well as the **higher technological** and **interconnectivity standards** demanded by the global market competitiveness, have **fostered further consideration of these services, mostly because of their ever growing economic and financial value**. Vast amounts of identity information are increasingly collected, aggregated, and used by different actors, both in the public and private markets. Amongst the latter there are the big technology platforms, which use this data to tailor commercial offerings. As reported by the EU Commission (and shown by LoginRadius data), this is the case for several digital market players, which enjoy substantial competitive advantages thanks to the amount of data they store, use and share with service providers[5].

[3]As well as Member States, eID schemes can also be notified by private sector providers as long as they are recognised by or provided on behalf of a Member State.
[4]Article 8 of the eIDAS regulation.
[5]LoginRadius: Digital Identity Trends (2019)

This **tailoring of the information** a person is exposed to, in turn, has a feedback effect that forms a person's opinions and ultimately can enforce or enhance properties of the person's identity.

The idea that EU citizens are not in control of their digital identity has led the EU Commission to **recognise the gaining of full control of identity information, as well as limiting its use and abuse, as one of the pillars of the agenda for Europe's future and of the Next Generation EU plan**.

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

On 9 March 2021, the European Commission presented a vision and avenues for Europe's digital transformation by 2030 proposing a **Digital Compass for the EU's digital decade** that evolves around four cardinal points - skills, government, business and infrastructures. On the digitalisation of public services, the objectives are 100% of key public services online, 100% of citizens having access to medical records, and 80% of citizens using digital ID.

Therefore, on 3 June 2021, the European Commission published a **recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework** and a **proposal for a regulation amending Regulation (EU) n. 910/2014 as regards establishing a framework for a European Digital Identity**.

The eIDAS Regulation, adopted in 2014, provides the basis for cross-border electronic identification, authentication and certification of websites within the EU, but does not require Member States to provide citizens and businesses with a digital identification system that enables secure access to public services or to ensure its use throughout the EU. The regulation also makes no provisions regarding the use of identification for private services or through mobile devices, leading to discrepancies among countries.

Therefore, starting from the consideration that the development of divergent national solutions creates fragmentation and deprives people and businesses from the benefits of the Single Market, as they cannot use secure, convenient and uniform identification systems across the Union to access both public and private services, the **recommendation underlines the importance to ensure that online service providers can rely on digital identity solutions recognised across the Union**, irrespective of the Member State in which they have been issued, thus benefiting from a harmonised European approach to trust, security and interoperability.

To this end, **the same recommendation encourages the strengthening of cooperation and the development of a toolbox, planned for September 2022, setting common standards and technical references as well as best practices and guidelines as a basis for the implementation of the European Digital Identity framework.** The toolbox should cover four cross-cutting dimensions, namely, the provision and exchange of identity attributes, functionality and security of the **European Digital Identity Wallets**, reliance on the European Digital Identity Wallet including identity matching, and governance with the eIDAS expert group being identified as the main interlocutor.

The proposal introduces a European Digital Identity Framework to **offer users self-determined personal digital wallets that would allow for a secure and easy access to different services**, both public and private, under the user's full control. In addition, **it aims to create a new qualified trust service for attestation of attributes concerning information related to identity, such as addresses, age, gender, civil status, family composition, nationality, educational and professional qualifications and titles, licenses, other permits and payment data, that can be offered, shared and exchanged across borders**, in full security, data protection and with legal effect across borders. The general goal is to respond to the dynamics of the markets and to technological developments, regulating three new qualified trust services - the provision of electronic archiving services, electronic ledgers and the management of remote electronic signature and seal creation devices. It will also offer an harmonised approach to security, for citizens relying on a European digital identity representing them online and for online service providers who will be able to fully rely on and accept digital identity solutions independently of where they have been issued. This objective is pursued through the passage from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid at European level.

Analysing the proposed changes, the regulation, after declining a series of definitions taking into account technological developments: a) **prescribes each Member State to issue a European Digital Identity Wallet within 12 months after the entry into force of the regulation**; b) **identifies permitted activities for users** (securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services and sign by means of qualified electronic signatures); c) **defines requirements of Digital Identity Wallets** (such as the provision of a common interface, high level of assurance, guarantee of unambiguous personal identification of the natural or legal person, impossibility for trust service providers of qualified attestations to receive any information about the use of these attributes and a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes); d**) prescribes Member States to provide validation mechanisms for the European Digital Identity Wallets** to ensure the possibility to verify authenticity and validity of the attestations and of attributed person identification data); e) **fixes that the European Digital Identity Wallets are issued under a notified electronic identification scheme of level of assurance 'high'** (free of charge to natural persons); f) **gives the user full control of the European Digital Identity Wallet** (prohibiting the collection of information not necessary for the provision of the service and prescribing that personal data relating to the provision of European Digital Identity Wallets are kept physically and logically separate from any other data held); g) **prescribes Member States to implement a common mechanism for the authentication of relying parties;** h) **allows for the Commission to establish a list of standards** for the certification of the European Digital Identity Wallets within 6 months of the entering into force of the regulation and enforce Member States to communicate to the Commission the names and addresses of the public or private certification bodies; i**) provides for the preparation and publication by the Commission of a list of certified European Digital Identity Wallets** based on information provided by Member States on European Digital Identity Wallet issued; l) **regulates cross-border reliance on European Digital Identity Wallets**, prescribing the acceptance of the European Digital Identity Wallet when the identification, or where strong user authentication is required by a public sector body, private relying parties providing services (including the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications) and very large online platforms (the Commission is called to encourage and facilitate the development of self-regulatory codes of conduct at Union level to ensure acceptance of electronic identification including European Digital Identity Wallets);

m) **regulates the mutual recognition of other electronic identification means;** n) **sets requirements for a qualified service for the management of remote electronic signature creation devices;** o) **regulates a qualified preservation service for qualified electronic signatures;** p) **fixes requirements for a qualified service for the management of remote electronic seal creation devices** and **for qualified certificates for website authentication;** q) **sets requirements for qualified electronic ledgers** (specifically, created by one or more qualified trust service provider or providers, ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger, ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry and record data in such a way that any subsequent change to the data is immediately detectable); r) **mandates Member States to collect** - and submit to the Commission by March each year - **statistics** in relation to the functioning of the European Digital Identity Wallets to be made available to the public (on the number of natural and legal persons having a valid European Digital Identity Wallet, the type and number of services accepting the use of the European Digital Wallet, incidents and down time of the infrastructure at national level preventing the use of Digital Identity Wallet Apps); s) **attributes the Commission the power to review** the application of the regulation and report to the European Parliament and to the Council within 24 months after its entering into force; t) **introduces new figures.** Among the most interesting, the **wallet provider**, who will be responsible for providing the technological support for the deployment of the system and for the aggregation of different certificates. Another key role is that assigned to the **providers of attestations** (certified and non-certified) who will help enrich the EUDI's value proposition and multiply its enhancement potential by issuing certificates that prove certain user attributes. These may be certified in nature, such as possession of a degree issued by one's university, but also non-certified, potentially including any badge or card we have in our wallet, such as a transportation card or loyalty cards.

The roadmap outlined by the Commission provides for the implementation of the digital wallet by 2023 through pilot projects to be in full swing by 2024.

Following the indicative timeline set by the recommendation, on 22 February 2022, the eIDAS expert group published the non-mandatory outline **"*European Digital Identity Architecture and Reference Framework*"** which provides a summary description of the eIDAS expert group's understanding of the EUDI Wallet concept, including objectives of the EUDI Wallet, roles of the ecosystem's actors, the wallet's functional and non-functional requirements and potential building blocks.

Considering that European Digital Identity Wallet will enable users to access online services, share data on them, and electronically sign/seal documents securely, the most significant use cases include secure and reliable identification to access online services, mobility and digital driver's license, health, educational certificates (diploma, degree, certificates, etc.) and digital finance. The document, specifically, describes the different roles of the EUDI Wallet ecosystem and highlights its multiplicity and complexity, both in the interactions among the various players and in the difficulty of coordinating and harmonising these roles in the generation, management and use of the data used and the functionality provided. The outline also describes the functional requirements of the EUDI Wallet based on the legislative proposal identifying functionalities divided into five categories - user interface, data storage, complex functions/cryptographic protocols, sensitive cryptographic material and eID means module.

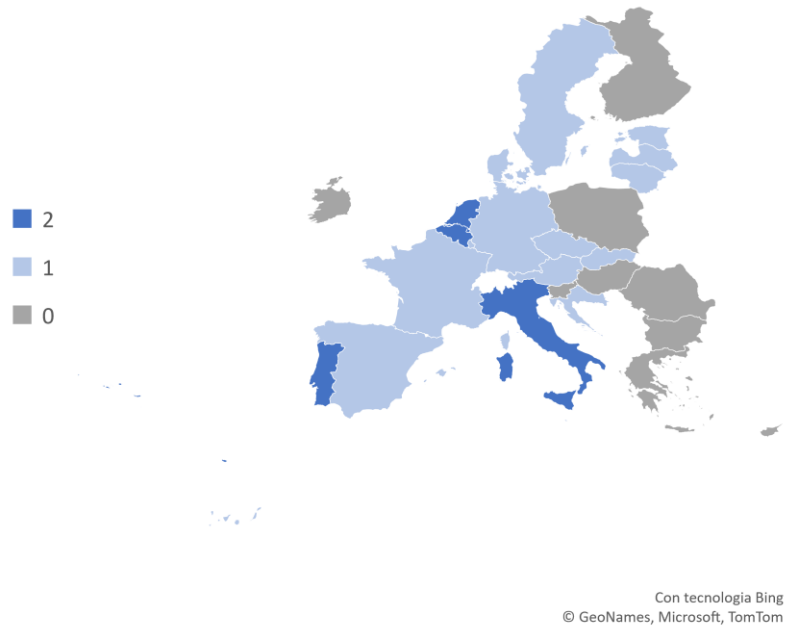
A lot of attention is placed on information. The user must have clear and unambiguous information about the operations they are performing in their activities, including the interaction with the various components involved. The attributes assigned to the user must be clearly indicated and the user must authorise their use for the specific operation (requiring the user to use two-factor authentication in a combination of at least two authentication factors for certain use case). For the implementation of the different functions of the EUDI wallet, they can be carried out using existing technologies such as a mobile application, web application, or PC-based secure application. Supporting building blocks are back-end server including the evaluated HSM for qualified signature, official electronic identity documents, secure external hardware token, cryptographic service provider and Trusted Execution Environment (TEE).

On 24 February, the Commission launched an online platform which will remain open to comments throughout the legislative negotiations and work on the toolbox, to make European Digital Identity Wallets a practical tool for all.
In the Parliament, the file has been assigned to the **Industry, Research and Energy Committee (ITRE)** which held a public hearing on the European Digital Identity Wallet and Trust Services on 3 February 2022.

2. An overview of the e-ID schemes in EU Member States

Since the entering into force of Regulation (**(EU) n. 910/2014)** in 2014, **18 Member States have notified at least one eID scheme and 4 Member States**[6] **have notified multiple schemes** for a **total of 22 eID schemes** registered so far. By September 2021, two other schemes[7] were being peer reviewed, while Portugal had pre-notified a third scheme.

Fig.1. Member States that have notified eID schemes under eIDAS (May, 2022)



Germany	National ID Card	Sept. 2017
Italy	SPID	Sept. 2018
	National ID Card	Sept 2019
Spain	National ID Card	Nov. 2018
Luxembourg	National ID Card	Nov. 2018
Estonia	ID Card	Nov. 2018
Croatia	eOI	Nov. 2018
Belgium	Citizen eCard	Dec. 2018
	Fas/Itsme	Dec. 2019
Portugal	National ID Card	Feb. 2019
	CMD-mobile	Apr. 2020
Czech Rep.	National ID Card	Sept. 2019
Netherlands	eHerkenning	Sept. 2019
	DigID	Aug. 2020
Slovakia	National ID Card	Dec. 2019
Latvia	eID Karte	Dec. 2019
Denmark	NemID	Apr. 2020
Lithuania	National ID Card	Aug. 2020
Sweden	Swedish eID	Dec. 2020
France	FranceConnect+	Feb. 2021
Malta	Identity Malta	Mar. 2021
Austria	ID Austria	Apr. 2022

Source: CEF Digital – Connecting Europe

Although most of these schemes are legally guaranteed by national authorities, which are responsible for setting up and aligning the eIDs with national legislation**, the distribution and provision of the identities is often left to authorised market players** (in certain cases, even several of such authorised companies for a single eID service), thereby favouring market openness and competition.

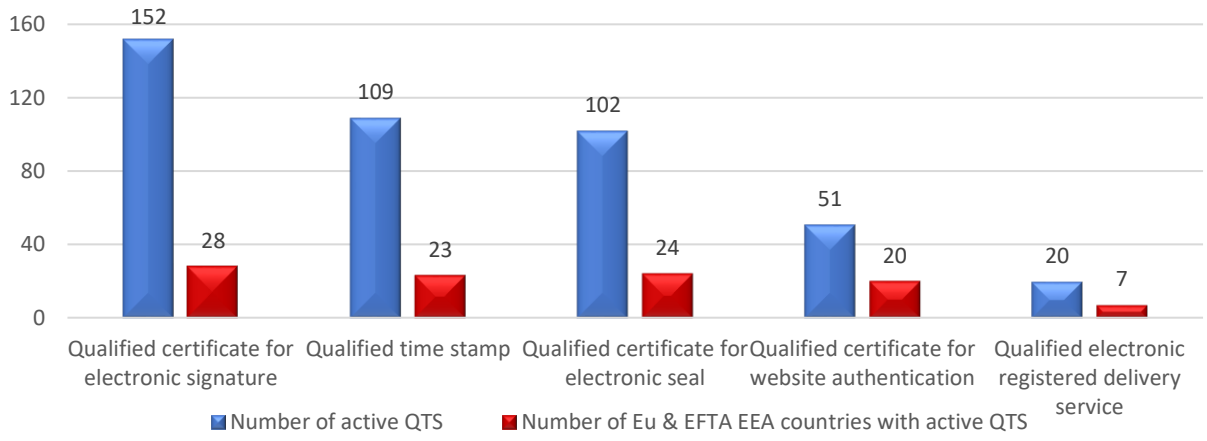
[6]Italy, Portugal, Belgium and the Netherlands.
[7]Norway and the Czech Republic.

Legal incompatibilities, technical interoperability issues, absence of national schemes, as well as lack of resources or political interest in notifying national schemes, have however led to rather low take-up rates within the Union. Overall, **the Commission highlights that only 14% of key public service providers across all Member States allow cross-border authentication with an e-Identity system**, although it also reports a **rise in the number of cross-border authentications**.

According to data recorded prior to the Covid-19 outbreak, **some countries had already reportede to have almost covered the whole population with the deployment of eIDs.** This is the case for **Estonia**, where more than 90% of the entire population was in possession of a digital identity, and with the **Scandinavian countries closely following** (all above 75% of adoption). Other countries, instead, had had much lower values, but then were forced to change due to the consequences of the pandemic. Amongst these, the **Italian** case offers an iconic example where, in 2018, only 3.6% of the population had a *SPID* eID, while in January 2022, instead, this share had risen to 47.4% as this instrument had become the key to many Covid-related national services (vaccination procedures, "Green Pass" certificates, access to financial aid and tax relief, etc.). Regarding the interconnection statuses of eIDAS cross-border functioning nodes[8], the EU Commission specifies that delays in the take-up derive from the absence of notifications from some nodes, while others are still in production, and not even fully operational yet[9].

[8]Cross-border authentications and the number of receiving transactions can be used as an estimate on the usage of notified eID schemes, as it is related to the number of use cases where citizens request access to an online service across borders.
[9]Most Member States are prioritising the development of the receiving capacity in their eIDAS nodes rather than the sending function.

Fig.2. The availability of Qualified Trust Services in Europe

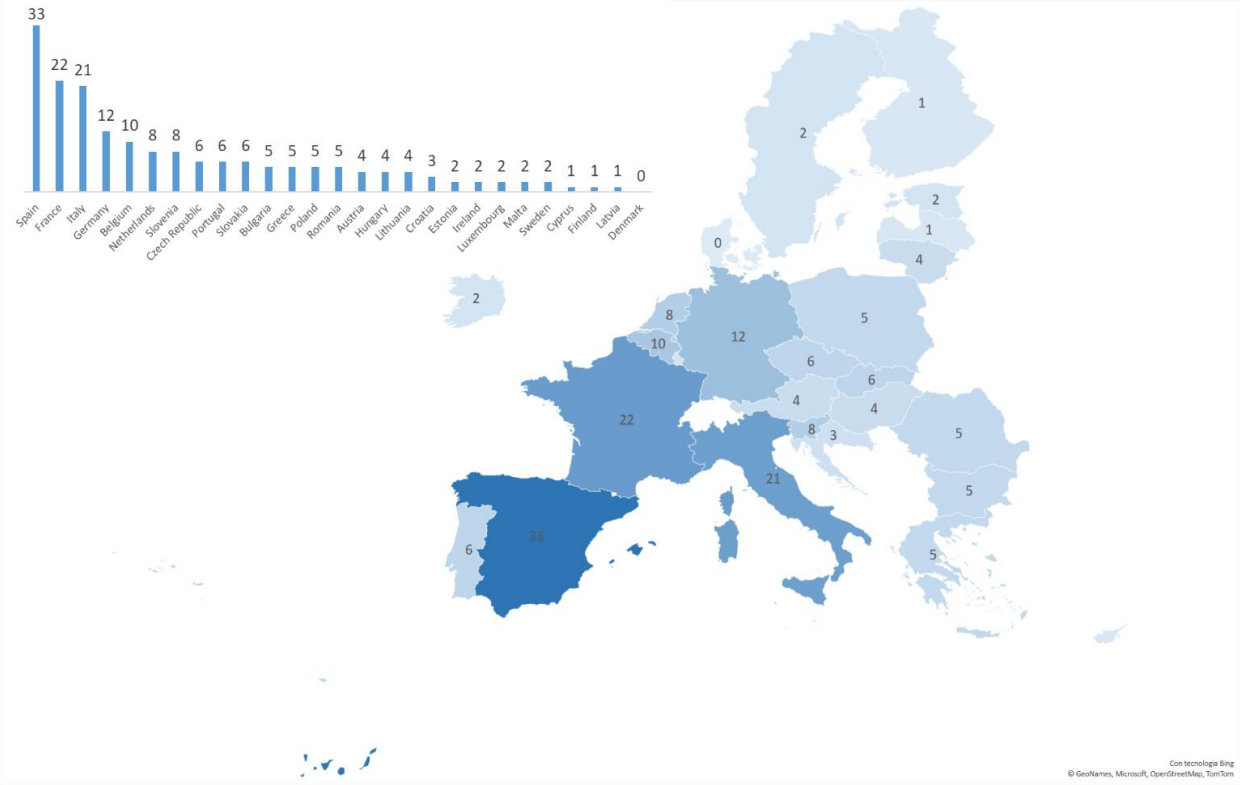


Source: European Commission - Impact Assessment (June, 2021)

Other **differences across countries concern the availability and provision of the different trust services** (QTS). **Qualified eSignatures are the type of service that are provided more often** (158 providers, available in 28 MSs), followed by qualified time stamps (109 providers, in 23 MSs) and qualified eSeals (102 providers in 24 MSs). Out of the core trust services, the qualified electronic registered delivery service is instead the most limited service, counting only 20 active services in seven Member States in March 2021.

A further constraint to a uniform application of the EU digital identity is represented by the **lack of a common interface**: during the authentication process users are in fact always redirected to the platforms of their national identity providers. This issue is particularly cumbersome in light of the fact that some countries do not only have more than one eID provider, but also several distributing channels – many of which are organised by authorised private-market companies - for such schemes and for the vast range of existing QTS.

Fig.3. Total number of Qualified Trust Services in Europe, per country



Source: European Commission - Impact Assessment (June, 2021)

According to the Final Report of the Study to support the impact assessment for revision of the eIDAS Regulation, carried out by PwC and DLA Piper, **in 2020, there were 180 Qualified Trust Service Providers (QTSPs) in Europe. The country with the highest number of QTSPs was Spain (33), followed by France (22), Italy (21) and Germany (12).**

In terms of **market value**, the Impact Assessment of the eIDAS Regulation does not provide any clear indications. The only available data that gives an idea of the existing Europe Identity Verification Market was provided in 2019 by ReportLinker. According to this study, in 2018, the total turnover for the eID market was €1.3 billion, a value **likely to have been significantly increased during Covid years**. Projected growth would reach **€3.8 billion by 2027**, representing a CAGR of 13.3% from 2018 to 2027.

Fig.4. Europe identity verification market 2018-2027* (in billion €)

Note: estimates
Source: ReportLinker FR- (November, 2019)

3. The benefits of e-ID

The eIDAS Regulation is a major step in building the European Digital Single Market and in boosting trust, security, and convenience around on-line digital services for governments, businesses and consumers. Thanks to eIDAS, the EU now has a predictable legal framework providing a means for **effective and secure cross-border authentication** through the mutual recognition of national eID schemes. With public services rapidly transferring to digital environments, there is a growing need to be able to access both national services and services from other EU Member States using a unique and secure eID. **Although the scheme still has some limitations in terms of full adoption and interoperability, it offers a series of benefits which are now widely recognised** not only in the public sector, but also among businesses and the general public.

Fig.5. eID facilitating interactions between individuals, businesses and institutions

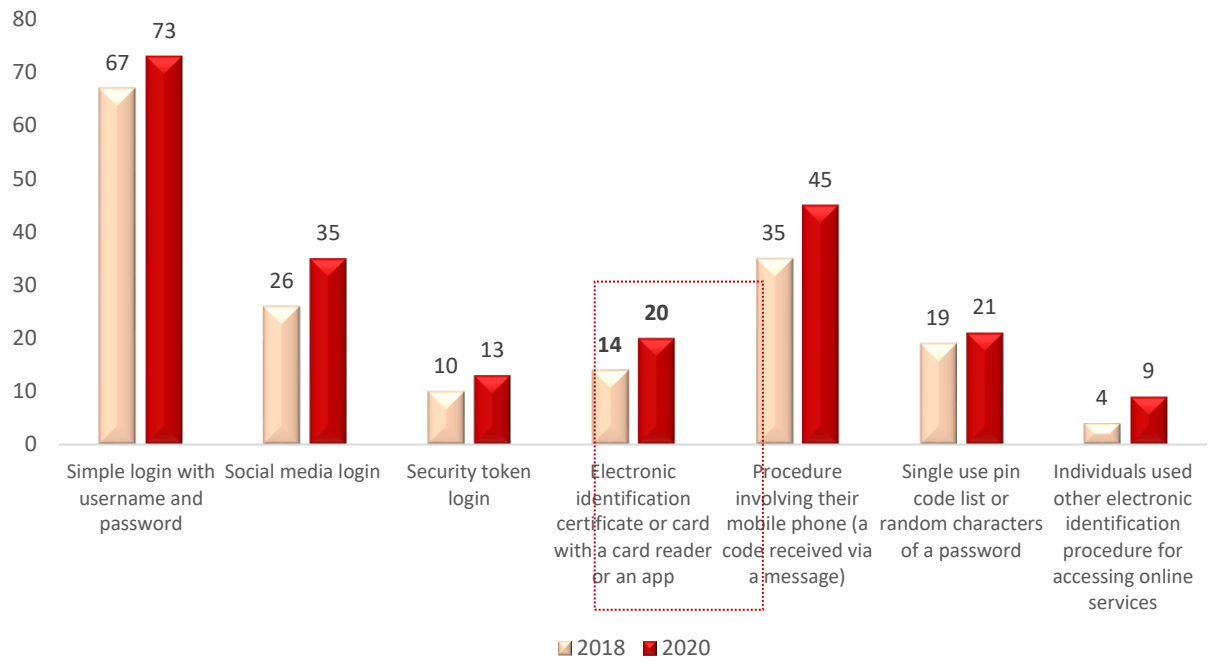
Source: McKinsey, 2019

One of the main benefits of using digital identity and trust services solutions is seen in the **increased level of security ensured by the common Levels of Assurance (LoA), included in eID schemes**, which lowers the risk of identity theft and misuse of personal information. These improvements increase the customers' **perception of a safe and reliable environment**, a matter which is of increasing importance especially for users concerned for their data privacy and control in certain sectors of the digital society (education, health, finance, etc.)[10].

[10]A recent Eurobarometer survey shows that 88% of consumers wish for more control over their data.

The uniform and interoperable system also improves **user experiences**, as managing multiple digital identities on different platforms - and with variable levels of data sensitiveness - has become a considerable burden for users, who are often asked to create a new digital login identity for each service they access.

Fig.6. Identification procedures used by individuals for accessing online services (%, EU-27 average)



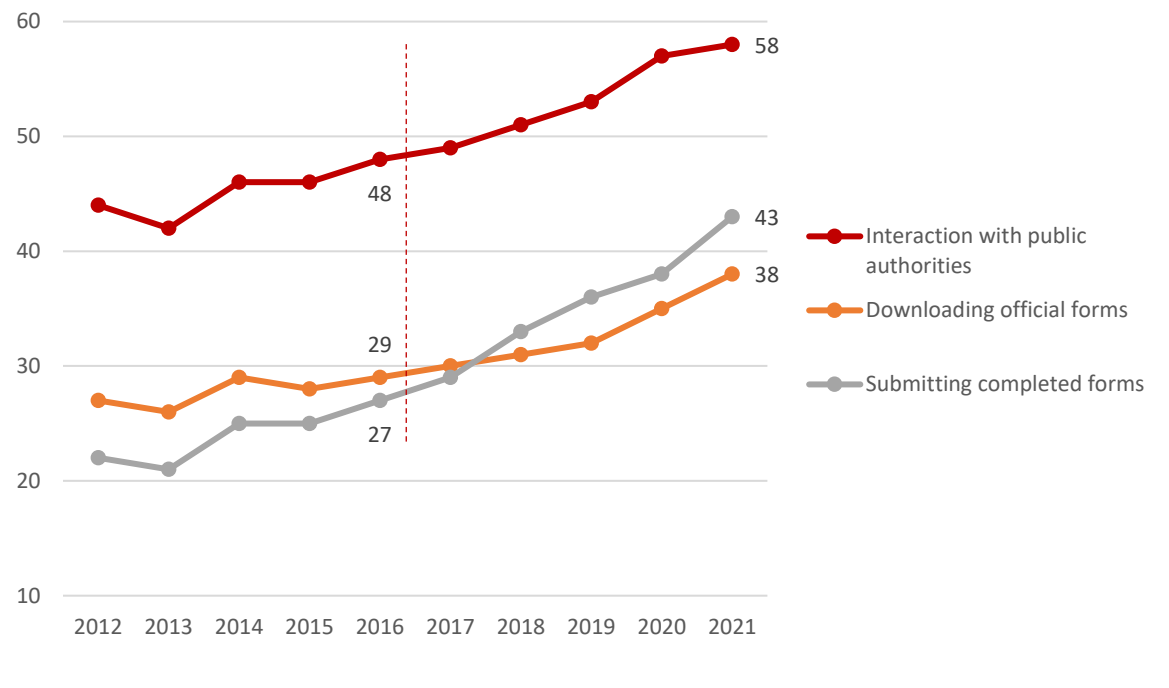
Source: Eurostat

Therefore, a single system of eIDs is of considerable importance, also in **improving accessibility** to such services, favouring inclusion with the ultimate aim of **making the benefits of the digital revolution easily exploitable for the whole population** and, in general, in better serving citizens, reliably, securely and transparently. The number of online accounts and the amounts of created data are rapidly increasing, with forecasts showing that, by 2025, the global datasphere will grow to 163 zettabytes, ten times the level in 2016[11].

[11]One zettabyte is equivalent to one trillion gigabytes. Data from The International Data Corporation.

As digital services increase in the number and types of activities involved, the management of a variety of usernames and passwords has become a major burden on private users[12], most having only started experiencing the transition to digital services during the recent Covid-19 pandemic. Although still low in comparison to other forms of log-in procedures, **electronic identification through eIDs has recently undergone a marked increase as preferred identification procedures** (Fig. 6), and, at the same time, European data also shows that **since the introduction of the eIDAS Regulation, European citizens have, on average, increased their eGov activities** (Fig. 7).

Fig.7. Trends in e-Government procedures (% of population who made use of such services, EU-27 average)



Note: The eIDAS Regulation was adopted in 2014, but it only entered into force in July 2016.
Source: Eurostat

[12]Nearly 50% of consumers have been unable to execute an online transaction due to forgetting their password (Ponemon Institute).

Associating virtual and physical relationships in the path to e-inclusion has in fact become a policy choice of the upmost importance, even in the public administrations. For example, secure and reliable digital technologies and IDs are **transformational in the provision and collection of bureaucracy-related forms** (i.e., tax forms, construction permits, certifications, authorisations, etc.), ensuring interoperability of processes and data protection in the migration from paper-based systems to digital forms of eGovernment services. In this perspective, technological improvements are also functional in enhancing **administrative efficiency**, reducing paperwork, speeding up processing, and reducing the risk of identity fraud. Digital IDs are also enablers for a safe and secure use of **e-health**, e-education, welfare payments, and working from home (WFH), key public services that have gained importance during the last two years.

In **an interoperable digital environment of trust and data protection**, these contribute to an increase in convenience for users, eliminating potential travel costs and minimising waiting times by allowing remote online authentication. Ensuring interoperability across private and public service providers domestically, as well as ID systems in other jurisdictions, is in this sense crucial, as it allows the certified eIDAS to exchange data with other systems, databases, devices, and applications. Going even further, the design of eGov services through the creation of more citizen-centric oriented services, together with the rethinking of the user experience processes of public services, are also triggering challenging questions in the role that eIDAS can have in supporting citizen participation, for example, through electronic voting, and in enhancing cooperation between the central states and local/regional authorities.

Such benefits are not only crucial for individual users of the digital environment, but also for the business sector, where transactions are made safer and more efficient thanks to the interoperability and the common standards. **eIDAS streamlines relations between governments and the private sector** in services including corporate registrations, taxes, economic support, permits, and authorisations, as well as favouring regulatory compliance and providing fraud-secure paths. Certified registration and authentication processes also support businesses by **making the digital environment safer**, a matter of great importance especially for industries that collect significant amounts of customer data, such as financial services.

The rise in the frequency of high-profile data security breaches[13] has indeed highlighted the need to guarantee secure authentication as technologies such as AI, IoT, blockchain and mobile technology, intersect to establish and verify identities. Facilitating private sector commerce in the digital age, and helping businesses carry out cross-border transactions, is a major goal of the eIDAS regulation, and both large and small businesses can make use of eIDAS in business-to-business and business-to-consumer transactions.

Through simpler process cycles, safer digital environments, and uniformed and faster task execution, companies face **substantial efficiency gains** and **lower costs** in the digital ecosystem. By increasing formalisation in authentication procedures, which helps reduce fraud, protects rights, and increases transparency, **companies do not only save on security expenses**, a financial burden which has considerably increased in the Covid-19 transition period[14], **but also on fixed costs** as service providers can communicate with their customers online with safety and confidence so as to reduce retail and brick and mortar expenses.

Overall, according to a 2019 McKinsey Report, **eIDs can also play a key role in the economy as a whole,** contributing significantly to the **creation of economic value for businesses** and the entire economic system **by enabling greater formalisation of economic flows**, promoting higher inclusion of individuals in a range of services, and allowing incremental digitisation of sensitive interactions that require high levels of trust. On average, the implementation of digital identity programmes could, therefore, lead to marked increases in GDP terms, with their forecasts suggesting that individual countries could **unlock economic value between 3 and 13 percent of GDP by 2030**[15].

[13]Data from recent years shows that cyberattacks have increased in both number and the value of economic damage. According to a study carried out by Comparitech in the third quarter of 2019, 9.68% of computers and 3.04% of mobile devices in the EU were infected with malware. The EU ranks first for the percentage of infected computers, ahead of China, Japan, the USA, South Korea and the UK.

[14]The latest version of the "Cost of a Data Breach Report" study, conducted by IBM, estimates that the average cost of violations globally was around $4.2 million in 2021. The economic repercussions on companies affected by cyberattacks have grown by 15% between 2017 and 2021, with a +9% only accruing to the latest year.

[15]It is important to highlight that these forecasts assume high level of adoption and the creation of economic value and strongly depends on the economic structure of the various countries: created economic value is equivalent to 6% of GDP in emerging economies but only 3% in mature economies. Source : https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

4. The European debate on the proposal

Even if the procedure is in its initial stage, some opinions have been expressed on the approach, aims and objectives pursued by the eIDAS Regulation. In particular, on 28 July 2021, the **European Data Protection Supervisor (EDPS)** gave formal comments on the Commission's proposal amending the regulation's content. Even if the EDPS welcomed the general approach to build on the existing legal act and increase the harmonisation of the EU level framework on digital identity and trust services, **it underlined that the technical implementation of the act will take place through secondary legislation** whereby it will be possible to **assess the compliance of the amended eIDAS with the GDPR only after the adoption of the implementing acts** laying down the technical specifications and reference standards. More specifically, the EDPS appreciates the clarification on the use of electronic ledgers, which are restricted to specific-use cases, supports the empowerment of the data subject and the principle of data minimisation, (prohibiting the issuer of the European Digital Identity Wallet from collecting information about the user to the minimum necessary) and welcomes the mandatory certification procedure of certain requirements for European Digital Identification Wallets. However, it recommends finding alternative ways to replace the proposed unique and persistent identifier, considering that it might cause issues with the GDPR and some national jurisdictions and underlines that the GDPR requires action from those in control functions no later than 72 hours after having become aware of a qualified data breach. Finally, the EDPS highlights that the prohibition to combine personal data from the above-mentioned sources with personal data from different types of services cannot be circumvented by contractual clauses or consent.

Following, the **Committee of the Regions (CoR)** and the **European Economic and Social Committee (EESC)** released opinions on European electronic identification on 12-14 and 20 October 2021, respectively. In the case of the **CoR**, it welcomed the Commission's proposal even if it identified some **technical risks stemming from the creation of centralised storage of identity data**, and underlined the importance of adequate safeguards against IT threats, data breaches and possible cyber-attacks, also suggesting the adoption of an authorisation check for eID access for economic operators based on a secured certificate with limited duration and subject to a regular renewal process. According to the CoR, use of the European Digital Identity Wallet should be voluntary, and the implementation of this system should ensure the development of adequate skills (especially in vulnerable groups, such as the elderly) and an effective protection of minors.

The **EESC** welcomed the Commission's proposal and the user centric approach adopted, underlining the importance to ensure inclusion through specific actions such as technological skills development for elderly users and other vulnerable groups and guarantee an effective protection of personal data. The EESC also stressed the need to align national legislation and EU-level acts regarding qualified electronic attestation of attributes and to guarantee compensation in situations of data loss or fraudulent behaviour independently of whether the provider is at fault.

Certainly, one of the most important issues in the European debate on the Digital Wallet, is the **protection of personal data,** essential for generating public confidence in the instrument and the proposing institutions. In particular, considering that the EUDI Wallet is also a container of personal data and that the exercise of "*full control*" over personal data by the user is hardly feasible, since the use of services is conditional on the provision of the same, some opinions have underlined the need for the user to know exactly what data flows into the wallet and how it is used (according to the principle of strict necessity) and have effective and efficient EUDI wallet recovery/locking procedures in case of loss, theft and failure of the technological device or smartphone.

Regarding the **actors** involved in the Digital Wallet implementation, the framework proposed by the European Commission identifies different roles within the ecosystem and new figures effectively creating new business opportunities, but actually gives **no indication as to which companies will preside over these roles**. This deficiency could create uncertainty in the players currently involved in the market for electronic identification services (trust service providers, banks, government agencies, for example) but also in new operators that potentially could be involved, thus, requiring the inclusion of more details and a clear legal definition of the various actors.

A **public hearing** on the proposal was held in the **ITRE Committee** last February and a wide-ranging debate is now predictably engaging stakeholders. At a general level, the committee's proposal introduces an entirely new, **highly complex model to be implemented in very ambitious time frames**. Considering the variety of functionalities to be aggregated, the **opportunity of proceeding in steps** has been noted, starting with the core functionalities on existing infrastructures arranging a progressive integration with the EUDI wallet as well as the **preservation of the separation between European (qualified) electronic authentication services and national electronic identification schemes for the time necessary for national authorities to establish these new schemes to avoid private authentication services not being established while waiting for the European Digital Identity Wallet to be agreed on by the 27 Member States (see below).**

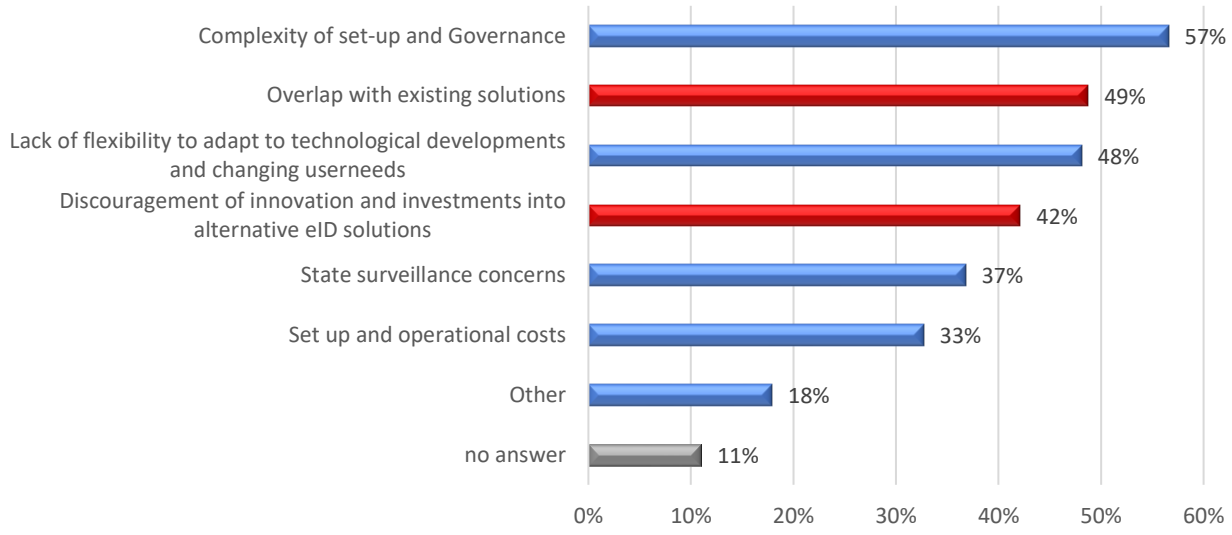
Another question regarding the general approach, also in a logic of risk-sharing, concerns the availability of two different instruments (one for public administrations and one for all other needs). In terms of **market impact**, the risk is that **the current proposal where authentication services are ancillary to national identification schemes and national European Digital Identity Wallets, eliminate a thriving market - that of authentication services -** with great potential, discouraging the seeking of accreditation by providers of attribute attestations and of authentication services before all national schemes are established.

5. The Public Consultation and the potential disadvantages of the regulation proposal

The regulation proposal was open to public consultation from July to October 2021, to **collect feedback** on the potential pros and cons of the development and uptake of both eIDs and other trust services in Europe, so as to evaluate the impacts that the several options concerning the delivering of the EU digital identity might have on markets and citizens. The aim of the consultation (that received 318 responses) was to **involve all interested parties**, specifically regarding public entities/national authorities, citizens, end-users, as well as companies directly impacted by the eIDAS Regulation such as trust service providers and identity providers. The latter are of particular interest as they offer a different point of view compared to that of citizens and general end users, providing important insights into the effects that these regulatory novelties may have in terms of competitiveness and market dynamics both at national and European level.

Together with a more general concern on the complexity involved in such a continental scheme in its setting up and programming stages, which is comprehensible and is to be expected when dealing with such radical initiatives, **most stakeholders have expressed worries on the potential disadvantages that a single and uniform European digital identity scheme might produce in terms of overlapping issues with existing solutions** (selected by 49% of respondents, Fig. 8).

Fig.8. Impact assessment for revision of the eIDAS Regulation: which possible disadvantages of such single and uniform European digital identity scheme are you concerned of?



Note. Respondents had the possibility to choose one or more preferences from the mentioned options.
Source: PwC and DLA Piper, Study to support the impact assessment for revision of the eIDAS Regulation. Final Report, April 2021

For example, this could be the case for the lack of a clear distinction between the ***identification procedures*** and the ***authentication procedures***, two apparently similar procedures, which nevertheless have certain specificities, key not only to the development of these technologies but also to the processing of personal data. Indeed, while a full personal identification (ID, passport, driving license, etc., and after the amendment of the eIDAS Regulation, the European Digital Identity Wallet) is needed when citizens interact with a public/private legal entity, in the interaction with platforms, websites, apps and other on-line services (carried out several billions of times daily) such entities have **no right to require full disclosure of personal identification data**. In the latter cases, only some attributes can be asked, meaning that *simple authentication procedures* are sufficient, and citizens should be made aware of such considerable differences, that are also specified in terms of citizens' and consumers' rights under Union law (GDPR, consumer protection, NIS 2Directive, etc.).

Therefore, to protect users from abuses and identity thefts, documentation and regulations should make **a clear distinction between identification and authentication,** while *"electronic personal identifications"* (or eIDs) are a way to prove unique identification of a person in a given context under the responsibility of Member States, *"electronic personal authentication means"* are ways to access online services and websites without necessarily disclosing personal identity.

A clear separation between European qualified electronic authentication services and national electronic identification schemes is also favourable for data protection issues, since there is currently an absence of a fair level playing field between notified providers according to Chapter II and qualified trust service providers according to Chapter III of the eIDAS Regulation. In fact, in the run-up to the publication of the NIS2 Directive, which should provide clarity on these issues, the security requirements and the conformity assessment procedures contained in Chapter III of the eIDAS Regulation are considerably more specific and demanding compared to the current requirements of Chapter II for electronic identification schemes. Furthermore, as highlighted by both the evaluation study and the impact assessment provided by the EU Commission, data protection issues are also raised by the fact that the way the identification schemes are regulated by the eIDAS proposal is incompatible with the so-called "zero-knowledge claims"[16], considered essential by the GDPR.

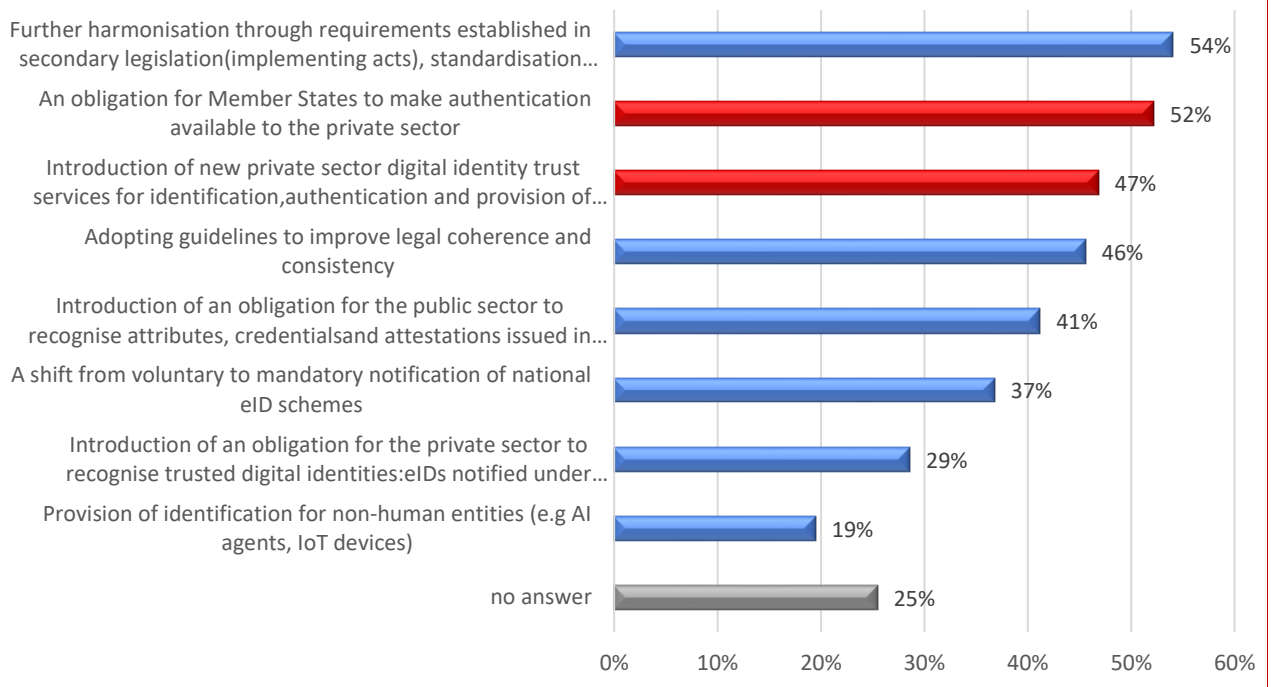
Concerns have also been expressed regarding the possible effects on competition and innovation, as well as for the considerable weight that governments will hold in such a uniform scheme. In fact, 42% of respondents believe that the proposed identity scheme risks producing "**discouragement of innovation and investments in alternative eID solutions**", while 37% feel uncomfortable with the state surveillance underlying the European scheme. The possible market structure produced by the new regulation could envisage the creation of 27 **national** (monopolistic *de facto*) **identity schemes**, with further market fragmentation and major differences compared to the set-up in use today. **In order to face the need for widespread and accessible digital e-Gov services, over recent years, several national authorities have made use of public-private-partnerships and of authorisation procedures involving private market players delegating the distribution and the releasing procedures of the required QTSs and eIDs to these entities**. This system, which is based on the inclusion of multiple players - both in the private and the public sectors - and which has not only favoured accessibility to such services, but also major efficiency and a variety of choice for citizens, will now be strongly affected by the European scheme.

[16]Such "Zero-knowledge claims" are privacy enhancing private services that can be provided by attribute attestation service providers (qualified and not) when users are interacting with private relying parties.

If even some Member States were to allow market competition in the identification scheme, **players could still become "*national champions*" also qualified as trust service providers.** Hence, it would be very likely for them to have an undue **competitive advantage** in the European market, **being, at the same time, qualified as trust service providers plus running a national identification scheme** (and a European critical infrastructure). In this market scenario, all other players would risk being in a disadvantaged position, and innovation could thereby be hampered as a whole.

Evidence of such concerns is also provided by the section of the Consultation in which stakeholders were asked to suggest corrective actions to be taken in the context of the revision of eIDAS to try to overcome the perceived shortcomings (Fig. 9). While 81 respondents did not provide any answers to this question, the remaining 237 reported, as the second and third best options, two issues related to the concerns the regulation's **impact on the existing private services**. Specifically, the option ***"An obligation for Member States to make authentication available to the private sector"*** **was selected by 52%** of respondents, while *"**Introduction of new private sector digital identity trust services for identification, authentication and provision of attributes**"* was chosen by **47%** of respondents, **highlighting that the perception of these issues is widespread among stakeholders**.

Fig.9. Impact assessment for revision of the eIDAS Regulation: which of the following corrective actions should be taken?



Note. Respondents had the possibility to choose one or more preferences from the mentioned options.
Source: PwC and DLA Piper, Study to support the impact assessment for revision of the eIDAS Regulation. Final Report, April 2021

6. Conclusions

The European Commission proposal, starting from the consideration that not all Member States offer an identification system to their citizens, and if they do, they do not always allow its use across borders and that the shift to the use of digital services has highlighted how the current system has limitations that need to be urgently addressed, aims to introduce a new model focused on the European Digital Identity Wallet. The latter, a personal digital wallet that should be built on the basis of trusted digital identities provided by Member States, would allow citizens to digitally identify themselves, store and manage identity data and official documents in electronic format.

The Commission will propose and agree with Member States on standards, technical specifications and operational aspects to ensure the Member States' Digital Identity Wallets have the highest security levels.

This is certainly an ambitious goal in a scenario characterised by a **great fragmentation and complexity**, where very different entities - public and private - operate clearly responding to different rationale. However, reaching this milestone is not a route without obstacles.

First of all, the overall European regulatory framework must be considered to **avoid any possible overlaps between the DMA, DSA and eIDAS,** which are not currently regulated, and to ensure a **coordination with the GDPR and cybersecurity regulation**.

With regards to the **roadmap**, the European Commission's proposal foresees a strict roadmap that should enable citizens to have the wallet by 2023. Given the complexity and variety of national contexts, the **opportunity of a phased approach should be evaluated**, also to **avoid market freeze,** pending agreement among Member States and the definition of national schemes.

Focusing on market impacts, the proposal does not properly address the distinction – indeed necessary - between **identification and authentication**. Considering that the former (identification) is an expression of the public powers of the state towards its citizens, while the latter (authentication) is intensively used for electronic services - that are partially included in the trust services as attribute attestation - the introduction of clear definitions maintaining the separation of the two concepts would perhaps be appropriate, as well as an additional thought to consider the impact on the authentication services market.

Concerns could also be expressed for what regards the possible effects on competition and innovation, as well as for the considerable weight that governments will hold in such a uniform scheme. Evidence of these concerns is also provided by the public consultation, with several stakeholders suggesting that the main corrective actions to be taken in the revision of eIDAS should involve an **obligation for Member States to make authentication available to the private sector** and to **introduce new private sector digital identity trust services for identification, authentication and provision of attributes**.

In light of the objectives pursued, the protection of personal data is crucial, making **high standards of transparency** essential for the data flowing into the wallet and its uses, the enhancement of the principle of strict necessity, and the provision of clear and effective procedures in case of loss, theft and failure of the technological device or smartphone (against abuse of dominant position, violation of fundamental rights, identity theft and digital addiction), as well as procedures for the **exercise of user rights** (first of all, the right to withdraw consent).