TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Natalia Vinogradova, Student code 192541IVGM

RE-SHAPING THE eIDAS REGULATION FROM STAKEHOLDER'S PERSPECTIVE

Master's thesis

Supervisor: Silvia Lips
LL.M, MSc

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Natalia Vinogradova, üliõpilaskood 192541IVGM

eIDASi MÄÄRUSE MUUTMISE PERSPEKTIIVID SIDUSRÜHMADE VAATENURGAST

Magistritöö

Juhendaja: Silvia Lips
LL.M, MSc

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Natalia Vinogradova

10.05.2021

Abstract

The EU Digital Single Market largely depends on its enablers: eIDs and electronic Trust Services. Therefore, the eIDAS revision is a part of the EU strategy, and its' revision requires a thorough evaluation involving all stakeholders to avoid further obstacles.

The study's primary purpose is to fill the gap in research, providing additional knowledge in understanding the obstacles and triggers of the EU digital identity implementations and giving recommendations in the further development of the eIDAS. The research explores the stakeholders' feedback on the EC Proposal (Inception impact assessment, 2020) to revise the eIDAS from 23 July 2020.

The research results suggest that the respondents see various challenges in the eIDAS implementation, and many are similar. Among mentioned obstacles are fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure, and excessive specialisation. Despite the similarities in perceived challenges, participants have different expectations for the eIDAS further development.

Keywords: eIDAS, electronic authentication, electronic identity, implementation challenges, identity management

This thesis is written in English and is 51 pages long, including 7 chapters, 13 figures and 1 table.

Annotatsioon

ELi digitaalne ühtne turg sõltub suuresti eID-dest ja elektroonilistest usaldusteenustest. Seetõttu on eIDASi määruse muutmine on osa ELi strateegiast. Lisaks määruse muutmine nõuab kõiki sidusrühmi kaasamist ning nende arvamuste põhjalikku analüüsimist ja hindamist selleks, et vältida edasisi takistusi eIDASi juurutamises.

Uuringu esmane eesmärk on täita lünk teadusuuringutes, pakkudes täiendavaid teadmisi eIDASi rakendamise tegurite ja takistuste mõistmisel ning andes soovitusi edasiarendamisel. Uuringus analüüsitakse sidusrühmade tagasisidet Euroopa Kommissiooni ettepaneku eIDASi määruse läbivaatamise kohta.

Uurimistulemused viitavad sellele, et vastajad näevad eIDASi rakendamisel erinevaid vaid sarnaseid väljakutseid. Nimetatud takistuste hulgas on killustunud tehnilised nõuded ja õigusraamistik, eIDASi ja kasutusjuhtumite piiratud ulatus, küberturvalisusega seotud küsimused, teavitamismenetluse keerukus ning liigne spetsialiseerumine. Vaatamata sarnasustele tajutavates väljakutsetes, on osalejatel erinevad ootused eIDASi edasisele arengule.

Märksõnad: eIDAS, elektrooniline autentimine, elektrooniline identiteet, rakendamise väljakutsed, identiteedi haldamine

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 51 leheküljel, 7 peatükki, 13 joonist, 1 tabel.

List of abbreviations and terms

C2B	consumer-to-business
C2G	consumer-to-government
EC	European Commission
eID	Electronic identification, electronic identity
eIDAS	Regulation (Regulation 910/2014, 2014)
eOI	Electronic Identity Card for citizens of the Republic of Croatia
EU	European Union
EUid	European Digital Identity
FAS	Federal Authentication Service (Belgium)
GDP	Gross domestic product
GDPR	General Data Protection Regulation
ICT	Information and communication technology
IoT	Internet of Things
LEI	Legal Entity Identifier
N/A	Data is not available
NGO	Non-governmental organization
NIAS	National Identification and Authentication System
NOBID	Nordic-Baltic Cooperation on Digital Identities
OJEU	Official Journal of the European Union
PPSN	Personal Public Service Number
QES	The Qualified Electronic Signature
SAML	Security Assertion Markup Language
SDG	Single digital gateway
SDGR	Single Digital Gateway Regulation (Regulation 2018/1724, 2018)
TOTP	time-based one-time password

Table of contents

List of figures

List of tables

1 Introduction

European Digital Single Market has a potential of boosting economic growth, bringing benefits to the private sector, consumers, and the public sector. According to the estimations, the digital economy has already contributed up to 8 per cent of EU GDP in 10 years, which equals Spain's GDP (EPC, 2010). The Digital Single Market operation largely depend on eIDs and electronic Trust Services. Citizens need to be able to use their national eIDs for the services in other EU member states. Meanwhile, there should be a guarantee that electronic Trust Services operate borderless inside the EU and be legally binding (Smiraglia et al., 2017). Overall, digital identity can create additional economic benefits, around three per cent in developed economies, provided the rates of adoption and use are high (McKinsey Global Institute, 2019).

Despite several initiatives in e-commerce at the beginning of 21 century, the EU digital market did not operate properly, had low cross-border online trade and ICT usage. The EU Member States had their individual digital markets that operated within the boundaries of national legal systems. For instance, the variety of identity solutions in the EU gradually became an obstacle to cross-border interoperability in the internal European market (Pelikánová et al., 2019; Tsap et al., 2020b). Besides the lack of interoperability, other barriers limited the functioning of the Digital Single Market, such as fragmentation and an increase in cybercrime (Polanski, 2015).

Consequently, the European Commission (EC) in its' strategy for 2014-2019 (COM/2015/0192 final, 2015) set three goals: improve access to online services, facilitate operation of digital services, maximise the growth of the digital single market economy (*Ibid.)*. Furthermore, new initiatives had to address those issues of fragmentation, lack of interoperability, and security. On 23 July 2014, the EC adopted the eIDAS Regulation (Regulation 910/2014, 2014; eIDAS regulation), thus repealing the outdated Directive 1999/93/EC *on electronic signatures*. The eIDAS aimed to establish a proper environment for the mutual recognition of "key enablers" and cross-border online government services in the EU, which included electronic identification, electronic signatures. This regulation would allow citizens to use their national electronic identifications in the other Member States to access electronic services, while businesses would operate cross-border smoothly (Regulation 910/2014, 2014). Some provisions of the eIDAS regulation were already in force since 2014, while some parts are applicable since 2016 and 2018. For instance, since 2016, the Member states could start voluntarily recognising e-Identifications (eIDs) of the other Member States. The eIDAS regulation is entirely in force since 2018, and the eIDs recognition process became compulsory for all Member States (Inception impact assessment, 2020).

1.1 Research problem and purpose

Since the eIDAS adoption, countries experienced several challenges in the regulation implementation process. For instance, some scholars indicate "compliance issues", "interpretation problems", "different practices in member states", "cooperation and collaboration barriers", and "representation of legal person challenges" (Lips et al., 2020). Therefore, the eIDAS regulation is under evaluation process right now. The EC published the proposal (Inception impact assessment, 2020) to revise the eIDAS Regulation. The stakeholders could give their feedback on the proposal from 23 July 2020 till 03 September 2020. In parallel, from 24 July to 2 October 2020 an open consultation was held to gather feedback on the implementation issues from the stakeholders. The public consultation was targeted to a wide range of stakeholders. This included European citizens, end-users, identity and trust services providers, public agencies, international organisations, and others affected by the eIDAS regulation (EC, 2020a).

Meanwhile, in October 2018 the European Commission (EC) adopted SDGR regulation, thus, establishing a framework for a single digital gateway (SDG) (Regulation 2018/1724, 2018). SDG should provide citizens and companies with information about national rules and administrative procedures as well as online services of all Member States. This will facilitate "the free movement of goods, services, capital and people" and single market operation (EC, 2021). The eID plays an important role in the creation of SDG, as it is mentioned, it is one of the "building blocks" that prepares the technical system for SDG (Regulation 2018/1724, 2018, p. 1–38, § 49). Furthermore, following the Digital Single Market Strategy for Europe, EC in its' new strategy for 2020-2025 aims to increase eIDAS efficiency and continue promoting digital identities (COM/2020/67 final, 2020).

Consequently, the eIDAS is a part of the EU strategy and its' implementation requires a thorough evaluation involving all stakeholders. Their feedback on implementation drawbacks and expectations for the eIDAS further development needs to be thoroughly analysed to become a base for future improvements in the framework.

For the time being, there is not much research on eIDAS implementation processes in EU countries, scholars studied mainly some specific areas or technical issues of the eIDAS (Lips et al., 2020). The study's primary purpose is to fill this gap in research, providing additional knowledge in understanding the obstacles and triggers of the EU digital identity implementations and giving recommendations in the further development of the eIDAS.

1.2 Research questions

Based on the research objectives in this study, the author tackles the following research question: How to identify the expectations of the stakeholders towards eIDAS regulation? Although the public consultation was targeted to a wide range of stakeholders, it is expected to have feedback mainly from two types of stakeholders: the member states officials and private sector representatives. Besides the author finds it important to determine, which problems are similar for all stakeholders, and provide possible recommendations for further development of eIDAS. Therefore, the main research question is split into four sub-questions:

1) How is the eIDAS Regulation perceived by the member states?

2) How is the eIDAS Regulation perceived by private sector organizations?

3) Which issues and problems are similar for all stakeholders?

4) What recommendations can be made for the further eIDAS review process based on the identified expectations?

The detailed methodology of the present research is provided in the second section of the thesis.

1.3 Overview of the thesis

Following the introduction, a detailed overview of the research design is introduced. Section three provides a literature review. Overview of the national eID systems and the eIDAS implementation in different Member States are outlined in the fourth part. Research results are described in the fifths section. The sixth section provides a discussion on the issues followed by a summary that concludes the topic.

2 Research design and method

The study's primary purpose is to provide additional knowledge in understanding the obstacles and triggers of the EU digital identity implementations and give recommendations in the further development of the eIDAS. The author aims at answering research questions by mapping the preferences of further development of the EU digital identity, as perceived by the stakeholders. In particular, the focus is on two main groups of stakeholders: the public sector representatives and private sector actors of the EU Member States.

Since the study embraces present-day phenomenon: the eIDAS implementation, moreover, the theoretical base is scarce, the strategy of the research is to conduct an exploratory case study (Yin, 2018) based on the feedback of the stakeholders. The EC conducted an inception impact assessment of the eIDAS revision and published a proposal to revise the eIDAS on 23 July 2020 (Inception impact assessment, 2020). In its' impact assessment, the EC proposes three options of the eIDAS revision. The first option foresees slight changes, including implementing acts and necessary guidelines and promoting eID under eIDAS to the private sector. The second option proposes a more extensive range of changes, including extending the regulation to the private sector and establishing new trust services. The third option would complement eIDAS with a European Digital Identity scheme (EUid) that the citizens could use for public and private services access. A combination of options is also possible (*Ibid.*). The feedback on the inception impact assessment was collected on 23 July 2020 - 03 September 2020 and was made available for the public on the European Commission website. Altogether 53 responses in different formats were received from various stakeholders. Some responses contained additional downloadable documents (EC, 2020b).

The collected feedback was extracted from the EC website with the help of the web scraping tool Scraper, meanwhile enclosed files were downloaded from the web pages. In total, it amounted to 156 pages of text. Some of the feedback needed to be translated from German, Spanish, and French into the English language for further analysis; therefore, Google Translate was used for these purposes.

After the data extraction, a thematic analysis of the collected datasets was applied to answer the research questions. The analysis was conducted in four rounds leveraging an interpretive research tool NVIVO that facilitates qualitative data analysis for academic purposes (QSR International, 2020). Firstly, the received feedback was sorted based on the theme from which country it was sent (Figure 1. Data analysis scheme).

Secondly, the data was split into three groups (case classifications: Stakeholders): the feedback from private, public organisations and others. Initially, it was expected to have the most responses from private and public organisations of EU Member States. However, the third sector organisations, EU citizens, and Non-EU organisations actively participated in the consultation. Consequently, three groups of cases were formed: stakeholders: public sector, private sector, and others (Appendixes 3 – 5).

The third-round task was to find a generalisation and central themes in each group of stakeholders (Appendixes 6 – 8). An inductive data-driven approach was applied to find patterns and probable explanations of the challenges and triggers of eIDAS implementation. During the final round, every pillar was analysed to identify similar problems and core issues for all stakeholders.

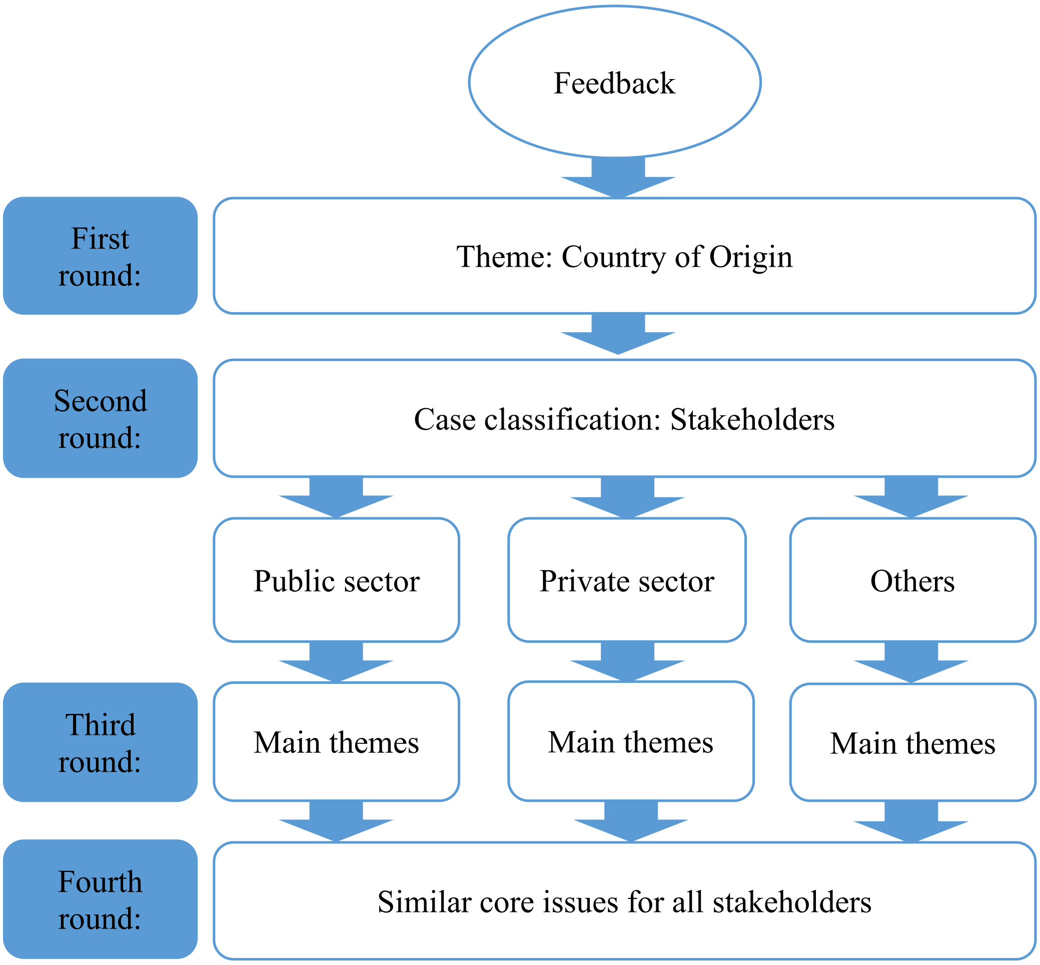


Figure 1. Data analysis scheme

The following section delivers a literature review on identity management and eIDAS issues.

3 Literature review

The electronic identity is a central concept for the development and operation of digital government (Khatchatourov et al., 2015; Tsap et al., 2019) and e-commerce (Neubauer & Heurix, 2010). For instance, the eID became a part of the Estonian critical infrastructure (Tsap et al., 2020b), and the state itself is the eID primary end-user and highly dependent on its eID (Valtna-Dvořák, 2020). Despite the importance of the concept, there is no universal definition for electronic identity. Literature indicates broad and narrow concepts of identity in the digital space. For instance, Hoikkanen et al. (2010) defines the term eIdentity as dataset related to a personal or collective identity stored and transferred in the electronic systems (Hoikkanen et al., 2010). It is worth mentioning that Hoikkanen et al. (2010) use the terms electronic identity, digital identity and eID interchangeably. At the same time, Khatchatourov et al. use the term eID only in the context of the eIDAS Regulation (Khatchatourov et al., 2015). Contrary, van Dijck and Jacobs specify eIDs as "digital solutions to prove one's identity", where the main functionalities of the solutions comprise authentication, login, and digital signings (van Dijck & Jacobs, 2020). Overall, identity in the digital space can relate to all online transactions (Khatchatourov et al., 2015). The present work focuses on national electronic identifications (eIDs), eID means, and trust services.

The topic of eIDAS implementation processes in EU countries is relatively new and partly researched. Mainly researchers focus on some specific areas or technical issues of the eIDAS (Lips et al., 2020). For instance, among technical solutions that are examined in the framework of eID systems and eIDAS: authentication of additional data and different cryptographic solutions (Morgner et al., 2016b), pseudonyms and pseudonymous signature (Khatchatourov et al., 2015; Kutyłowski et al., 2016), and integration of blockchain technology with Qualified Electronic Signatures (Turkanovic & Podgorelec, 2020). Further, there are proposals to widen the scope of the technological solution, for example, including an electronic signature of the ICO smart contracts (Veerpalu et al., 2020).

Furthermore, the literature analyses the national eID systems, their integration with eIDAS-Node, their further extensions, proposes alternative technical solutions. For instance, the German eID schema is broadly examined (Kutyłowski et al., 2016; Morgner et al., 2016b, 2016a). Further, an overview of the Italian architecture for the eIDAS-Node and connection of the eID scheme is provided (Smiraglia et al., 2017), and the Dutch IRMA eID system is outlined (van Dijck & Jacobs, 2020).

Some scientists offer various applications of the eIDAS-node in the educational context (Alonso et al., 2020; Berbecaru et al., 2019; Gerakos et al., 2017; Klobučar, 2019). For instance, some studies propose an extension of the basic set of attributes by adding academic attributes as part of citizens' profiles and offer technical solutions. They claim that it would be beneficial for citizens in the education context. In particular, this would save the students' time on the application procedure and allow them to use academic services through national eID (Alonso et al., 2020).

Since the provision of online services is closely related to the concerns of "security, privacy, and trust" (Al-Khouri, 2014) moreover, a multitude of various digital identities brings inconveniences for users and endangers their security and privacy in cyberspace (Neubauer & Heurix, 2010), privacy aspects are widely discussed in the context of electronic identity, identity management, and eIDAS (Khatchatourov et al., 2015; Kutyłowski et al., 2016; Morgner et al., 2016b). For example, Kim Nguyen considers aspects of trust that are embedded in the eIDAS regulation. Firstly, he argues that the certification procedure guarantees users that the provider's services are trustworthy. The requirements for the trust services provision, the systems itself and its' elements are established in the European standards. Moreover, the certification is provided by independent third parties and supervised by national agencies. As a result of certification, all qualified trust service providers are registered in the trust lists together with the description of their services. Other criteria that would ensure trust by Nguyen are the evaluation of the cryptographic process, the definition of minimal requirements, and decentralized trust models based on transparency principles (Nguyen, 2018).

Some scholars investigated if eIDAS is beneficial for the Member States and their national cross-border programmes and e-government objectives or somewhat burdensome. Although eIDAS poses additional obligations on the Member States, they suggest that it rather supports national initiatives and projects, such as E-residency in

Estonia, than challenges them. Therefore, it is beneficial for the governments to implement eIDAS (Aavik & Krimmer, 2016).

Nevertheless, initial research on eIDAS implementation indicates that some countries are more successful in their endeavours while others are hesitant and struggle with the eIDAS implementation, especially those less experienced (Pelikánová et al., 2019). Early comparison of national eID systems in Europe demonstrates that there are different technical and organisational elements between the systems (Kubicek & Noack, 2010), architectural solutions of the identity systems are diverse (Khatchatourov et al., 2015). The reason for this diversity can be clarified by the fact that each EU Member State developed their eID management systems independently (Smiraglia et al., 2017), based on the earlier systems and during "incremental innovation" and "path continuation" (Kubicek & Noack, 2010). Each country tried to meet its' internal goals to provide secure authentication, while "interoperability with other state's eID schemes was no priority" (Ribeiro et al., 2018). Nevertheless, identification and authentication systems of different EU countries have many similarities (Roelofs et al., 2019).

The diversity of the rules and systems in the electronic identity management between countries caused issues with interoperability and turned out to be an obstacle for cross border electronic services and operation of the EU Digital Single Market (Ribeiro et al., 2018; Smiraglia et al., 2017). Generally, information systems operate on identities that connect citizens with the digital information stored in the databases. If identifiers in different databases vary, cross-referencing the information from one database to another is hindered. Therefore, the main challenge for identity management is to adapt the systems, making them interoperable and enabling cross-referencing and matching the information (Backhouse, 2006). In other words, Member States need to implement national gateways, called eIDAS-Node, to connect to the eID systems of the other Member States (Smiraglia et al., 2017).

Besides interoperability issues, some authors suggest that the difficulties with eIDAS implementation might be caused by the complexity of the eID concept, which encompasses more than outlined by the EU frameworks. Meanwhile, the legislation concentrates mainly on technical and legal interoperability; other issues of a political and social nature may cause conflicts and obstacles for the eIDAS implementation. For instance, in the case of the Swedish national eID schema, it was challenging to design a new eID system having, at the same time, already existing BankID and considering opinions of all the stakeholders involved (van Dijck & Jacobs, 2020).

Overall, the main challenges for the member states indicated in the literature are “compliance issues”, “interpretation problems”, “different practices in member states”, “cooperation and collaboration barriers”, and “representation of legal person” challenges (Lips et al., 2020). Besides, the lack of knowledge among users influences the citizens' adoption rate of national eID solutions, which negatively affects the consumptions of cross border electronic services. Therefore, countries should increase awareness among citizens about national eID solutions and their benefits and provide them with necessary software and qualified certificates (Roelofs et al., 2019). Since eIDAS implementation is a relatively new topic in research, it requires further research. The proposed endeavour attempts to gain knowledge of the obstacles and triggers of the EU digital identity implementations from the stakeholders' perspective.

4 Background

A notion of identity is an old concept (Hoikkanen et al., 2010) that has been mainly related to face-to-face identity management. Traditionally, a passport served as an identity verifying tool in the face-to-face identity era. Passports were issued by the state authorities and were used for cross-borders travels, the nation's security, and surveillance purposes. Besides, a person could verify one's identity with the passport while applying for various services provided by the state or businesses (van Dijck & Jacobs, 2020). However, digital technologies changed identity management drastically, transferring it to the digital area (Hoikkanen et al., 2010; Stevens et al., 2010). One of the main distinctions of electronic identity from the traditional concept is that people can have different identities in the digital world and use them depending on the circumstances in various information systems.

Moreover, the amount of identity systems is constantly increasing (Hoikkanen et al., 2010; Neubauer & Heurix, 2010). Besides national eID solutions, corporations actively provide their customers with electronic identities to facilitate their electronic services. For example, among the leading technologies that the corporations use are Open Authorization (OAuth), OpenID, and Windows CardSpace and U-Prove project. Open Authorization (OAuth) technology is used by many corporations, mainly social media organizations. OpenID is supported by a non-profit foundation, while Windows CardSpace and U-Prove project are both produced by Microsoft (Buccafurri et al., 2018).

Some authors argue that these various digital identities bring inconveniences for users and endanger their security and privacy in cyberspace (Neubauer & Heurix, 2010). Further, the increasing cases of cybercrimes prompted discussion on cybersecurity in the digital and electronic identities ecosystems. Some authors suggest that governments should take a leading role in developing digital identity management, thus building trust in digital services (Al-Khouri, 2014). Meanwhile, others argue that “banks could and maybe should play a more active role in this space” (Salmony, 2018).

Initially, the Member States developed their electronic identities and trust services on their own depending on the requirements and circumstances. Although some international standards advanced, for example, SAML, and were applied by many EU countries, the implemented local rules and practices in each country are different (Smiraglia et al., 2017). Besides, the adoption rates of the national eIDs vary from country to country. The issues of trust, privacy, and security are often suggested as influencing factors for the eID acceptance by the citizens of a country (Tsap et al., 2019). For instance, in Estonia, more than 2/3 of citizens routinely use national eID. From the citizens' perception point of view, the main reasons behind such widespread use are convenience, speed, security, and availability of various authentication tools that can be chosen depending on the circumstances (Tsap et al., 2020a). Other studies consider cultural issues as major influencing factors to the eID and eGovernment solutions adoption (Al-Hujran et al., 2011). The following subsection details the national eID systems of the EU Member States.

4.1 Overview of the national eID systems

Austria

Since 2009 there are two alternative citizen cards available in Austria: eCard as a Citizen Card and a Handy-Signatur mobile phone card. Since 2016 the mobile phone signature is available in the form of a mobile app (Joinup platform, 2020l). Electronic governmental services in Austria can be accessed on the online portal Oesterreich.gv.at with the help of a mobile phone signature - Handy-Signatur, EU Login, and a new ID Austria solution (Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2021b). New project ID Austria (the electronic proof of identity) further develops the previous citizen card/Handy-Signatur solution. The main changes concern the registration procedure, extra attributes, and service-providers accreditation (A-trust, 2021). The project is in the pilot or testing phase till autumn 2021. As soon as the pilot project is finalized, the Handy-Signatur will be replaced by the ID Austria. The new ID Austria card will be issued to all citizens from the age of 14 together with a passport. Moreover, foreigners will be able to apply for their ID Austria card at the local police department (Bundesministerium für Digitalisierung und Wirtschaftsstandort, 2021a).

Belgium

Belgium pre-notified the EC about its eID Scheme FAS / eCards on 28 May 2018. The peer-review process took around seven months, and the eID scheme was notified with a level of assurance 'high' on 27 December 2018 (eID User Community, 2019a). The

Belgium eID scheme consists of the Federal Authentication Service (FAS), the Belgian Citizen eCard and the Foreigner eCard. FAS and the Belgian citizen eCard systems operate since 2003, while Foreigner eCard since 2006. All Belgium citizens are obliged to obtain the Citizen eCard from the age of 12. In 2017 the FAS managed around 43 million authentications (Smeets, 2018). In addition to the eID Scheme FAS / eCards, on 18 April 2019, Belgium pre-notified the EC about its new eID Scheme FAS / Itsme®. The itsme® mobile App scheme received notified status in the OJEU on 18 December 2019 with a high level of assurance. The Belgian Mobile ID NV/SA provides login services and mobile app, while the registration is based on the Belgian eCards (Smeets, 2019).

Bulgaria

In 2020, in Bulgaria, 26,9% of persons used the Internet for interaction with public institutions. 19% received information from governmental websites, 15% submitted applications, declarations and reports, and 14,4% downloaded documents, forms, and other documents (MTITC, 2021). Overall, these indicators are below the EU average. Meanwhile, the national electronic identification scheme is under construction in Bulgaria. Electronic governmental services can be accessed via Egov.bg portal or on the websites of the agencies and ministries. To identify oneself on the portal, a person needs to choose an eID provider out of the three options: authentication with QES (The Qualified Electronic Signature), Cloud QES B-trust, and Cloud QES Evrotrust. The cloud electronic signature was launched in 2019 as a mobile ID. Besides, there are several other means of electronic identification in use that are issued by various agencies, such as: "National Revenue Agency, the National Social Security Institute, National Health Insurance Fund" (Joinup platform, 2020m).

Croatia

Croatian National Identification and Authentication System (NIAS) operates since 2013. NIAS passed the notification process on 7 November 2018 and received a high level of assurance. eID carrier is a personal identity card (eOI), which the Ministry of Interior issues. eOI is supplied by the state-owned agency – AKD (eID User Community, 2018). In addition to the notified scheme, there are around 23 authentication means within NIAS. Some of them are operated by governmental organizations, some of them by private companies, others with mixed funding. However, those means are not in the process of notification (Roelofs et al., 2019).

Cyprus

A Cyprus national electronic identification scheme is under construction, and legislation needs to be harmonised with the eIDAS regulation (Joinup platform, 2020n). Two governmental web portals cyprus.gov.cy and eservices.cyprus.gov.cy (Government Gateway Portal Ariadni), provide information about governmental electronic services. E-services for the citizens are accessible on the Ariadni portal after registration and profile identification through electronic banking (Department of IT Services, 2021a, 2021b). The first trust service provider JCC Payment Systems received authorisation in February 2019 (Joinup platform, 2020n).

Czech Republic

The Czech Republic eID scheme was notified on 13 September 2019 with a high level of assurance. The eID cards are issued to Czech citizens and mandatory from the age of 15. However, the activation of electronic identification is voluntarily (Ministry of the Interior of the Czech Republic, 2018). Alternatives to the eID cards that provide access to the governmental e-services a "combination of username, password, and one-time codes" (Joinup platform, 2020j), Mobile key of eGovernment, national EU ID, login with Starcos smart card, mojeID, and Bank Identity (Ministry of the Interior, 2020). However, the alternative options to the eID cards are not notified to the EC so far.

Denmark

Denmark takes an active part in the Nordic-Baltic Cooperation on Digital Identities (NOBID) project, which aims to provide interoperability of the national eID infrastructures and access to digital services for citizens and companies within the Nordic-Baltic region. The citizen portal borger.dk was launched in January 2007. It contains information about all the governmental layers: national, regional and local, and provides e-services of the public sector and sign-in solution (Joinup platform, 2020k). Danish eID scheme is named NemID and was notified on 8 April 2020 with a substantial level of assurance. eID means are comprised of several solutions, such as, various key cards and tokens, hardware, and mobile application. NemID is widely used by the citizens having

5,16 million users and almost 60 million transactions per month. Governmental digital mailbox is obligatory for all citizens, which can be accessed only via NemID (Agency for Digitisation, 2019). Currently, NemID is going through a modernization phase with a new supplier and will be substituted by the MitID (Agency for Digitisation, 2021).

Estonia

Estonia launched its first national eID cards in 2002. The card is the primary identification and travel document within the EU and obligatory for Estonian citizens from 15 years old and foreigners who live in the country (Joinup platform, 2020a). Besides the citizens' eID cards, several other authentications solutions are used (eID User Community, 2020b). All those six eID systems were notified on 02.11.2018 with a high assurance level. The ID card, the diplomatic card, and the RP card identify both in physical and digital worlds, while Digi-ID, Mobiil-ID, and e-Residency ID are only digital eID means. Mobiil-ID can be activated with the person's ID card or RP card. The responsibility for the scheme is split between authorities. Some services, such as manufacturing and personalization, are outsourced to private companies. All those identification systems can be used to access both governmental and private companies services (eID User Community, 2019b). Furthermore, a Smart-ID application is in operation in Estonia, but the scheme was not notified. This application was developed purely by the private sector and belongs to SK ID Solutions AS (Information System Authority, 2021).

Finland

Most electronic authentications in Finland are performed utilising bank eIDs (90%). National eID cards are used mainly for physical identification and only on rare occasions (1%) for online identification. Around 9% of all online transactions are performed with the help of eIDs issued by mobile operators. National eIDs for citizens and foreigners permanently residing in Finland are created together with a personal identity code. Finland intends to work on new digital identification solutions and reform the personal identity codes system, which in use already since the 1960s (Joinup platform, 2020b). Currently, to access public e-services, citizens and foreigners need to identify themselves on the portal Suomi.fi choosing one out of the offered identification tokens. This includes online banking codes, certificate card, mobile certificate, Finnish Authenticator app, and European identification tokens. A certificate card comprises an identity card issued by the police, an organisation card, an ID card for regulated social welfare and healthcare professional, and a healthcare smart card issued by the Digital and Population Data Services Agency. Finnish Authenticator app is a new means of identification and intended for foreigners (Digital and Population Data Services Agency, 2021). Finland has not yet started the pre-notification procedure of eID schemes under eIDAS (eID User Community, 2019a).

France

There are various suppliers of public identities in France, such as a tax department, social security and postal services providers, mobile operators. It was decided to develop a FranceConnect platform that would allow a single sign-on solution for public services. It was planned that public electronic services providers and 30 private companies would join the platform, which was launched in 2016. Further work on the identification solutions continued, and the programme on the development of a digital identification system in France was launched in 2018. By March 2020, the FranceConnect platform had already 15 million users. Users can access digital governmental services on the Service-Public.fr portal (Joinup platform, 2020c). France started the pre-notification procedure of eID schemes FranceConnect+ / The Digital Identity La Poste under eIDAS on 2 February 2021 (eID User Community, 2021a).

Germany

First German national eID cards were issued in 2010, which replaced a conventional ID card. Besides being a physical identity document, the new eID card allowed users to authenticate online. The decision to develop an eID strategy in Germany was taken the following year. Despite the availability of new functionalities, the new eID was not used online widely among the citizens. Therefore, in 2017 the government issued the Electronic Identification Promotion Act and took some additional measures. Concerning the notification process of the German eID scheme under eIDAS was started and finalised on 26 September 2017 with a high level of assurance. Germany was the very first country which notified European Commission about its' national eID schemes (Joinup platform, 2020d). The eID means under the notified scheme initially were National Identity Card and Electronic Residence Permit (eID User Community, 2019a). In 2019 Germany introduced an additional electronic ID card for the EU and the European Economic Area citizens (Joinup platform, 2020d). The notification was updated in the OJEU on 14.12.2020 (eID User Community, 2019a). The governmental portal bund.de was revised in 2018. The users of the portal can access electronic governmental services through a federal service account. Further, it is planned to connect subnational and regional portals with the federal portal (Joinup platform, 2020d).

Greece

In 2019 Greece started developing of the public administration portal gov.gr, which was launched in 2020. The portal provides public electronic services for the citizens. To access the services, citizens should use credentials of the online tax and customs services portal TAXISNET (Joinup platform, 2020e) or online bank (Ministry of Digital Governance, 2021). Currently, the Greece National Authentication project is under development (Joinup platform, 2020e).

Hungary

National eID cards were launched in 2016, and by 2020 five million eID cards were issued. Besides the eID cards, Hungarian citizens use other electronic identification solutions, including the Client Gate trusted profile and telephone authentication. The Central Client Authentication Agent - identity-checking agency service - started its' work in 2016, supporting various electronic identification and authentication solutions. Electronic governmental services can be accessed on the National Portal (Joinup platform, 2020f) after identification using one of the four options: national eID card, Client Gate account, phone identification, and a new option - facial identification (NISZ Zrt, 2021). The eIDAS authentication is under development. Besides, Hungary has started preparations for the pre-notification procedure of eID schemes under eIDAS (Joinup platform, 2020f).

Ireland

Governmental portal gov.ie covers all the necessary information about governmental services in Ireland. The portal was recently revised and updated with information from the departmental websites. However, to access electronic governmental services, citizens use various identification solutions and portals. For instance, Personal Public Service Number (PPSN) is used identify citizens by the Department of Employment Affairs, the

Health Service Executive, the Revenue Commissioners. Further, the Public Service Card authenticates an identity to access public services, including electronic services. The card has already been issued to around 3.2 million people by the year 2020. Department of Social protection manages a relatively new MyGovID system that allows access to various services (Joinup platform, 2020g). A user of the MyGovID can create a basic account or verified account. A basic account requires only the user's name and an email address. A verified account is more secure, provides a wider range of services and requires a basic MyGovID account, a phone, personal public card number, and a public services card (Department of Social Protection, 2021). By February 2020, MyGovID has around 470000 verified accounts.

Furthermore, since 2015 Irish Tax and Customs department provides online access to its' services on the MyAccount website (Joinup platform, 2020g). A user needs to register oneself on the site or continue entering the services with a verified MyGovID (Revenue Irish Tax and Customs department, 2021). The development of Ireland's trust services infrastructure is in progress to be in line with the eIDAS requirements (Joinup platform, 2020g).

Italy

Italian SPID – Public System of Digital Identity - was notified under eIDAS on 10.09.2018 and amended twice afterwards (eID User Community, 2019a). Citizens can obtain a digital identity from one out of nine identity providers by registering at their websites (Agency for Digital Italy, 2021). Identities differ by level of assurance: low, substantial, and high (eID User Community, 2019a). In 2019 already 4000 governmental organisations provided their electronic services through the SPID system (Joinup platform, 2020h). By 28 February 2021, all governmental institutions should switch their authentication solutions to the SPID system. Moreover, private organizations can adopt the system as well (Agency for Digital Italy, 2021). In 2019 more than 5 million citizens used the SPID system and obtained an eID (Joinup platform, 2020h). Furthermore, on 13 September 2019, Italy finalized the notification procedure of its' second eID scheme: Italian eID based on National ID card, with a high level of assurance (eID User Community, 2019a). Italy started working on the eID card project already in 2001. As soon as the testing phases were finalized, eID cards are being issued to all citizens older than 15 years old (Joinup platform, 2020h).

Latvia

Latvian eID system includes various identification means, incorporating eID card, qualified electronic signature, mobile solutions, and eAddress accounts (Joinup platform, 2020i). The Concept for Latvian Electronic Identification Cards was approved on 12 January 2010. The first eID cards were issued in March 2012. At first, the eID cards were voluntarily obtained; however, it was decided in 2016 that the eID cards should be mandatory for the whole population of Latvia and activation of the qualified electronic signature certificate (Joinup platform, 2020i). In 2019 Latvia renewed its' eID cards that have new security features and an unlimited number of e-signatures (Public broadcasting of Latvia, 2019).

Another identification solution - the eSignature portal - was registered in 2018. The portal was developed by VAS Latvijas Valsts radio un televīzijas centres (State Joint Stock Company Latvian State Radio and Television Centre) and allows signing documents electronically (Joinup platform, 2020i). Moreover, it provides several electronic tools such as eParaksts in eID card (eSignature in eID card), mobile application eParaksts mobile, and eParaksks card for legal organizations (VAS "Latvijas Valsts radio un televīzijas centrs", 2017).

Citizens can access government services through the State and Local Government Services Portal latvija.lv. The portal provides access to 122 eServices and 672 external eServices (Joinup platform, 2020i). There are ten authentication tools available to access electronic services, among them: eID card, mobile authentication, iBanking, eSignature, and eIDAS (State Regional Development Agency, 2021).

Latvia notified European Commission eID schemes under eIDAS on 18 December 2019. The information was published in the official journal the same day. Registered eID means include eID Karte, eParaksts Karte, eParaksts karte+, eParaksts, which have a substantial and high level of assurance (eID User Community, 2019a).

Lithuania

In 2008 Lithuania amended the law on Identity Cards, allowing national identity cards to be used for identification purposes in an electronic environment. Since then, Lithuanian citizens could sign documents electronically (Joinup platform, 2020o). The Lithuanian

National Identity card (eID / ATK) scheme was officially notified to the European Commission on 21 August 2020 (eID User Community, 2019a). Overall, there are three Lithuanian and one Estonian trust service providers active in Lithuania (Joinup platform, 2020o).

The eGovernment gateway portal was launched in 2004 and revised in 2015. It provides information about governmental services for citizens and businesses in a life events format. Access to the electronic services amounted to over 603 in 2019 (Joinup platform, 2020o). To access the governmental electronic services, visitors of the portal need to choose a user type (citizen or residents, business, service provider) and authenticate with bank ID, with electronic identification device or with a Google account. The electronic identification devices include ID card and reader, mobile devices, USB or card and reader. Foreign citizens can authenticate themselves using the eIDAS option (Information Society Development Committee, 2021).

Luxembourg

Web portal for citizens and enterprises Guichet.lu was launched firstly on 17 November 2008. In 2019 new functionalities were added to the portal. Now it provides, besides governmental information, access to electronic services for citizens through MyGuichet.lu. Electronic authentication certificates, such as LuxTrust Token, ID Card, Smartcard, or Signing Stick, provide security during electronic transactions and a possibility to sign electronic documents (Joinup platform, 2020p). A LuxTrust Scan and LuxTrust Mobile tools were recently added to MyGuichet.lu to facilitate access through a smartphone and an electronic device that generates a one-time password. Moreover, redirection to the eIDAS node is activated that allows the use of digital identities from another EU Member State (Ministry of Digitalisation, 2021a).

Luxembourg national identity card (eID card) scheme was notified 7 November 2018 (eID User Community, 2019a). Although ID cards are mandatory for all citizens aged 15 and over except those living abroad, activation of the electronic certificates is voluntarily (Ministry of Digitalisation, 2021b). National electronic signatures are managed by LuxTrust S.A. that provides a central electronic Identity infrastructure and solutions based on personal authentication certificates in Luxembourg. The LuxTrust products are used by public and private companies, including the banking sector (Joinup platform, 2020p).

Malta

Governmental online services in Malta can be accessed through an e-ID Single Sign-on Account. It is possible to subscribe to the account with an e-ID card or e-Residence Permit card. After receiving the card, a user needs to activate an eID account to use electronic services (Identity Malta Agency, 2021). The e-ID cards are issued to Maltese citizens 14 years of age and older. The signature certificates can be provided to those who are 18 years and older. Foreign residents in Malta are eligible for e-Residence cards with the same e-ID features (Joinup platform, 2020q).

An overview of the governmental services can be found on Servizz.gov.mt. The portal is integrated with the eForms platform that distributes received forms to the appropriate government organization (Joinup platform, 2020q). Individuals can sign in to the Servizz.gov.mt portal entering an ID Number and a password (Servizz.gov Agency, 2021). Those services that require a high assurance level of authentication can be accessed with the ID card and PIN. Services with a substantial level of assurance have a "two-factor authentication mechanism on a time-based one-time password (TOTP)" (Joinup platform, 2020q). Ultimately, Malta started the pre-notification procedure of its' Identity Malta schemes on 04.03.2021. Maltese eID card and e-residence documents are the eID means under the scheme (eID User Community, 2021b).

Netherlands

There are public and private providers of trust services in the Netherlands. The main authentication solution for citizens is DigiD, which is a public authentication solution. For example, 663 governmental organizations provided electronic services through the DigiD system, and more than 340 million DigiD authentications were performed in 2019 (Joinup platform, 2020y). There are four levels of assurance for DigiD authentication: basic, medium, substantial, and high. The basic level includes username and password and is called DigiD. Medium assurance can incorporate either DigiD and SMS-authentication or the DigiD app. Substantial assurance is the DigiD app with an ID verification (ibid.). A high level of assurance is achieved by using new certificates on ID cards issued from the 13th of March 2021 (Logius, 2021). DigiD scheme with substantial and high levels of assurance was notified to the European Commission on 21 August 2020 (eID User Community, 2019a).

Another Dutch eID scheme, Trust Framework for Electronic Identification, was developed especially for businesses and governmental organisations. To use the authentication token of the system, a user needs to be an authorisation from its' organisation. The solution is used less than the DigiD, 441 public organisations provided services through the system, and around 9.2 million authentications were performed in 2019 (Joinup platform, 2020y). The Dutch Trust Framework for Electronic Identification was notified 13 September 2019 (eID User Community, 2019a).

Poland

Five qualified trust service providers operate in Poland, which offers qualified electronic signatures, electronic seals, and time stamps, validates signatures and seals, and issues qualified website authentication certificates (Joinup platform, 2020r). For instance, every citizen can create a personal online account on login.gov.pl, so-called a trusted profile. Login.gov.pl was launched on 09.09.2018. The profile allows using electronic government services and signing electronic documents on the national portal Gov.pl (Novak, 2018). Activate profile is possible via online banking or e-ID card (Ministry of Digital Affairs, 2021b). Foreigners from Croatia, Estonia, Spain, Lithuania, Luxemburg, Portugal, Slovakia can also log in to the portal with their national e-ID cards (Ministry of Digital Affairs, 2021a).

The first e-ID card in Poland was issued on 4th March 2019. Since then, an e-ID card allows authenticating in case of online services, for instance, while accessing Portal Gov.pl, and to sign electronic documents (Ministry of Digital Affairs, 2020). Some electronic services can be accessed with the help of a Mobile app; by February 2020 the number of application users reached 600 000.

Portugal

Digital Identification management in Portugal characterizes constant changes and modifications. Electronic Citizen Card was introduced in Portugal on 5 February 2007. However, the activation of the electronic signature feature stays optional and is only for citizens over the age of 16. In June 2017, the law on the Citizen Card was changed, and the Professional Attributes Certification System was integrated. Thus, it became possible to use e-signature by specific professionals (Joinup platform, 2020s). Instead of having several documents, such as identity document, taxpayer document, voter card, it is enough to have a citizen card that incorporates all the documents in one (Administrative Modernization Agency, 2021b).

An alternative authentication system was introduced in 2014, the Digital Mobile Key that works in governmental websites. In 2017 new features were added to the system and variations of digital signing. Moreover, citizens could access their data stored in governmental registries. Further, professionals could use the Digital Mobile Key for electronic signing (Joinup platform, 2020s).

The ePortugal.gov.pt was launched in 2019, making it possible for citizens and businesses to interact with governmental organizations and use electronic services more efficiently (Joinup platform, 2020s). To use the services on the portal, an individual needs to create an account. User authentication is possible through a digital mobile key, citizen card, or digital certificate. The latter option is only for the professional activities of the notaries, layers, solicitors (Administrative Modernization Agency, 2021c). Besides those three authentication methods, some governmental websites allow other authentication options, such as username and password, social account (Facebook, LinkedIn, Twitter), eIDAS (Administrative Modernization Agency, 2021a).

As for the notification procedures of eID schemes under eIDAS, on 30 May 2018, Portugal pre-notified its eID Professional Attributes Certification System to the European Commission. The system comprised of the Portuguese CC eID card, CMD scheme (online digital identity service), and SCAP scheme (online digital identity service). On 28 February 2019, Portugal finalised notification procedures for its' Portuguese national identity card (eID card) scheme. Later, the Digital Mobile Key eID scheme was notified on 8 April 2020 (eID User Community, 2019a).

Romania

Romanian National Electronic Identification system is still in the development phase. In 2020 a project "Centralised Digital Identification Software Platform" was launched (Joinup platform, 2020t). It is decided to finalize the project by 31 August 2023 (Authority for the Digitalisation of Romania, 2021a). Currently, there are only several governmental services that are available online. For instance, the National Electronic Payment System for Taxes provides electronic services (Joinup platform, 2020t), where citizens can authenticate with their bank cards (Authority for the Digitalisation of Romania, 2021b).

Slovakia

Slovakia issues two types of eID cards: electronic citizen and electronic residence cards. Electronic citizen cards are for Slovak citizens of 15 years old and above. Electronic residence cards are for residents of Slovak Republic (eID User Community, 2020a). First eID cards in Slovakia were issued in December 2013, which replaced conventional identity cards and allowed the electronic signing of documents. However, electronic signature functionality was optional. Since September 2018, to receive electronic services, foreigners can log with an ID or a residence card on governmental websites.

Moreover, since February 2019, it is possible to log in with eIDAS as a resident of an EU member state (Joinup platform, 2020u). For example, the national platform Slovensko.sk provides governmental electronic services, can be accessed with Slovak ID or as a resident of an EU member state (National Agency for Network and Electronic Services, 2021). Slovakia finalised notification of its' eID scheme under eIDAS on 18 December 2019 with a high assurance level. The eID means under the scheme includes Slovak Citizen eCard and Foreigner eCard (eID User Community, 2019a).

Slovenia

First national projects on authentication and trust services in Slovenia were launched in 2015. Trust Service Authority of Slovenia offered a new Authentication and eSignature Service SI-PASS solution in 2017. Since then, SI-PASS was implemented in many governmental systems (around 30) (Joinup platform, 2020v). SI-PASS can be used for verifying the identity of citizens, businesses, and officials. SI-PASS enables authentication with digital certificates, SI-PASS user name and password, mobile identity smsPASS, Social accounts (Google, Facebook and Microsoft user account), and EU authentication means (Trust Service Authority of Slovenia, 2020). In 2018 became possible through SI-PASS to use mobile phones for authentication and signing electronic documents. By 2020 around 15 governmental systems integrated the smsPASS option (Joinup platform, 2020v).

Slovenia plans to introduce new identity cards that could be used in the electronic environment for identification purposes. New legislation in this area is under a process of adoption. Furthermore, a new app for mobile identification is under development (Joinup platform, 2020v).

Spain

Since 2014 Spain uses a common electronic identification system - the Cl@ve system - in all governmental electronic services. The system allows two types of identification: based on two keys and based on digital certificates (Joinup platform, 2020w). The keys (username and password) can be temporary that is valid for a short period or permanent (for a long yet limited period). Every access to e-services through Permanent Cl@ve requires, besides fixed keys, a one-time key sent by SMS. Moreover, permanent Cl@ve allows cloud-based signing of electronic documents (Government of Spain, 2014). The second type of identification, which is allowed by the Cl@ve system, is based on digital certificates, including electronic ID. It is also applied to the cross-border recognition system eIDAS. By December 2019, already 7606 organizations adopted the Cl@ve system, and 172 million transactions were performed during 2019 (Joinup platform, 2020w).

The first national electronic ID cards in Spain were issued in 2006. In 2015 new version of the card, which combines the latest security measures and the latest identification technologies, was approved (Ministry of the Interior, 2021). In 2020 it was issued around 38 million Spanish eID cards (Joinup platform, 2020w). The Kingdom of Spain notified its' eID schemes under eIDAS with a Spanish ID card on 7 November 2018. The level of assurance was assigned as 'high' (eID User Community, 2019a).

Sweden

Sweden introduced national electronic ID card on 1 October 2005, which is not mandatory and does not substitute paper ID cards. Besides national eID cards, other electronic ID cards and "mobile/computer-based" eIDs are widespread in Sweden. This includes BankID, Freja eID+ and Telia, issued by various providers and facilitates access to some electronic governmental services (Joinup platform, 2020x). For instance, Verksamt.se that provide government services for businesses, can be accessed through Swedish e-identification and foreign eID. Swedish electronic identification can be processed through BankID and Mobile BankID, Telia, Freja on the portal (Swedish Companies Registration Office, 2021).

To implement the eIDAS, Sweden takes part in the "Nordic-Baltic eID Project" (NOBID) (Joinup platform, 2020x). Currently, the eIDAS infrastructure is implemented by Sweden, and a connection is available with five EU countries. Moreover, around 180 governmental organizations provide cross-border authentication solution (Joinup platform, 2020x). Furthermore, Sweden started pre-notification of its' eID schemes under eIDAS with eID means: BankID and Freja eID, on 14 December (eID User Community, 2019a).

In short, the national eID systems vary significantly within the boundaries of the EU. Some countries have been providing their citizens with electronic identifications for years, while others have just started working on the solutions. Consequently, the rates of eID adoption differ from country to country. Since the eIDAS adoption, the Member States gradually started notifying their eID schemes. The list of EU member States that pre-notified and notified eID schemes is given in Appendix 2. The following subsection elaborates on the eIDAS implementation status.

4.2 The eIDAS implementation status

The eIDAS regulation grounded the legal foundation for electronic transactions in the EU internal market. The aim was to build trust among consumers, businesses, and public authorities in the digital environment, thus boosting electronic commerce and increasing the effectiveness of public and private digital services in the Union (Regulation 910/2014, 2014). Compared to the previous Regulation 1999/93/EC on e-signatures, the new regulation provided unified rules for all Member States and had a much broader application framework. Firstly, it became possible to recognise other national electronic identification systems developed in the Member States (Polanski, 2015). Thus, it facilitates access to cross-border electronic public services in other EU countries through national electronic identification tools (eIDs) (EC, 2020c). Secondly, new types of trust services were added, and uniform requirements for Trust Services were established (Polanski, 2015).

Although the eIDAS was approved on 23 July 2014, it was entering into force step by step. European Commission defines five stages of the eIDAS regulation entering into force (Figure 1. Timeline of the eIDAS entering into force). From 29 September 2015, the member states could start voluntarily recognising eID means of other members. In early 2016, eID interoperability infrastructure became available for the states. From July 2016, provisions referring to trust service rules became effective. Finally, from 29 September 2018, the member states are obliged to recognise the eID means of each other mutually (EC, 2019).

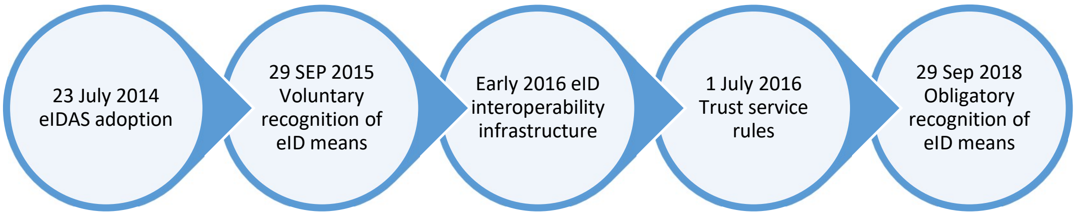


Figure 2. Timeline of the eIDAS entering into force. Source: (EC, 2019)

The eIDAS implementation comprises several stages that each country should follow. Firstly, a member state should start eID pre-notification: officially inform the European Commission about its "intention to notify its eID scheme". Then a peer-review stage follows, where representatives of other Member States examine the eID scheme. After the peer review stage, the country notifies the European Commission about its eID scheme. As soon as the information about notification is in the Official Journal of the European Union (OJEU), but not later than 12 months, other Member States should recognise the notified eID scheme. Since the recognition, EU citizen can use the recognised eID across borders (EC, 2019; eID User Community, 2019a).

Germany was the first country, which in 2017 notified other member states about its' eID scheme and presented for recognition. The following year Estonia, Spain, Croatia, Belgium, Luxembourg, and Italy followed Germany (eID User Community, 2019). From

November 2019, the national eID schemes from six EU countries could be used across borders. These countries included Germany, Italy, Estonia, Spain, Luxembourg, Croatia (EC, 2019). At the moment, 14 Member States out of 27 passed the process of notification of their eID schemes, and three countries (Sweden, Malta, France) pre-notified the European Commission (eID User Community, 2019a, 2021a, 2021b) (Appendix 2).

Initially, it was planned to revise the eIDAS regulation and its implementation process by 01.07.2020 (Regulation 910/2014, 2014, § 49). In the Strategy (COM/2020/67 final, 2020) published in February 2020 *on Shaping Europe's Digital Future*, the Commission confirmed its intention. The EC conducted an inception impact assessment of the eIDAS revision and published a proposal to revise the eIDAS on 23 July 2020. In its' inception impact assessment, the EC proposed three options: 1) revise and slightly update the current regulation, 2) extend the effect of eIDAS to the private sector, 3) launch a European Digital Identity (EUid) or combine these three solutions (Inception impact assessment, 2020). The feedback on the inception impact assessment was collected from 23 July 2020 till 03 September 2020. The following section provides an overview of the respondents' expectations towards eIDAS implementations and further development.

5 Research results

During the first round, the collected datasets were analysed, leveraging a thematic analysis based on the theme from which country the feedback was received. Altogether, 53 responses from 16 countries were presented on public consultation, conducted by the European Commission from 24 July to 2 October 2020. The first round of the thematic analysis of the extracted data showed that among the respondents were representatives of the non-EU countries (Switzerland, UK, USA, Norway), which constituted 19% of all respondents. Some respondents preferred to preserve their anonymity; therefore, the data about their countries of origin were not available (N/A) (Figure 3. Respondents by country of origin (%)).

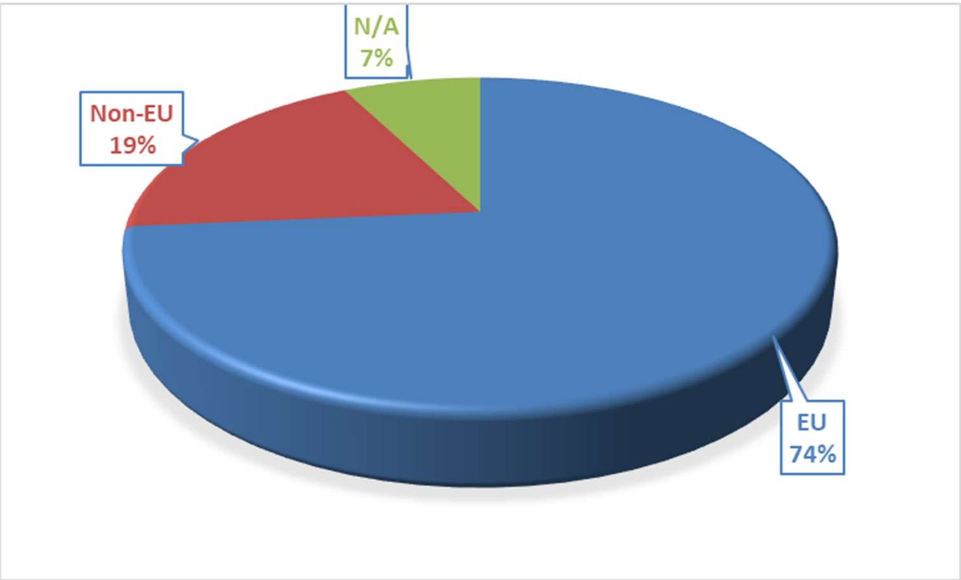


Figure 3. Respondents by country of origin (%)

The largest number of respondents were from France (12), then followed by Germany (7), Belgium (5), and the USA (5) (Table 1. Respondents by country of origin).

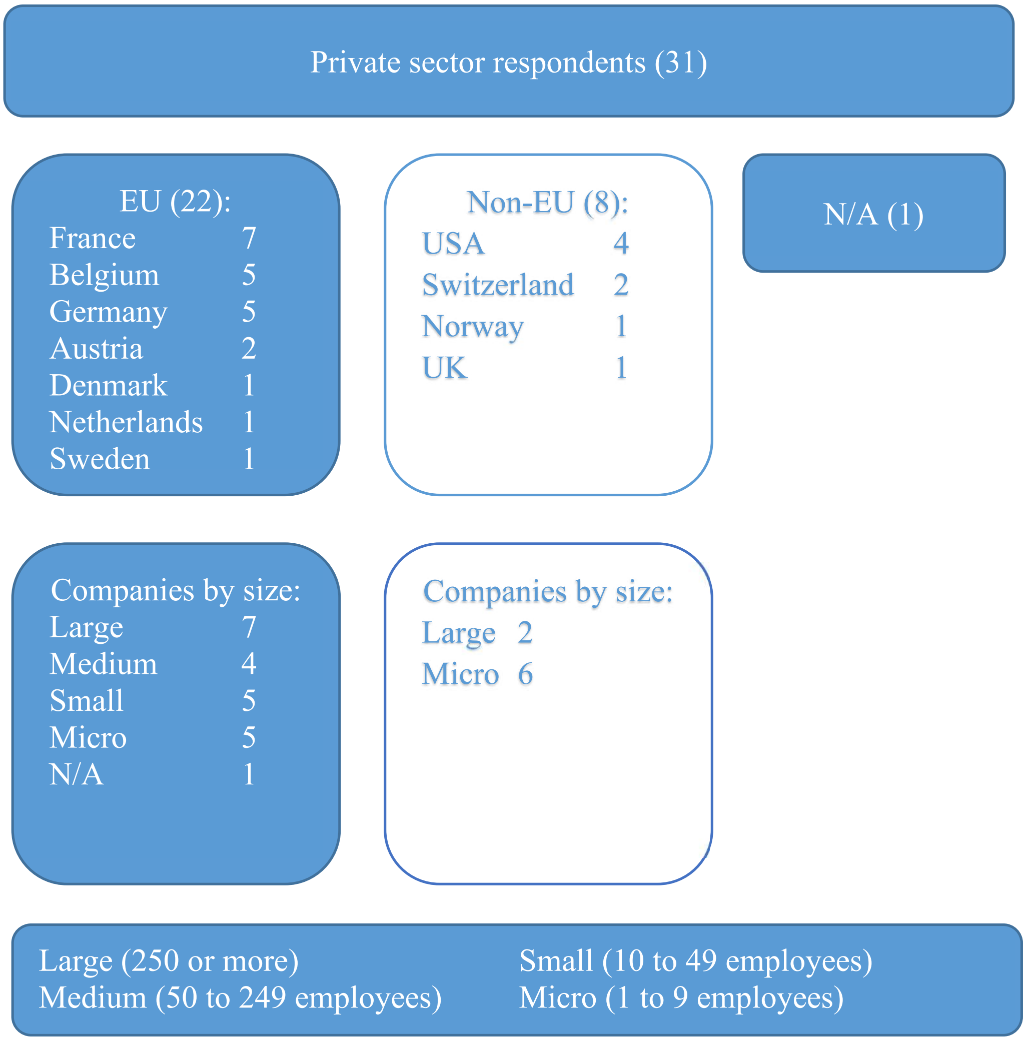
Table 1. Respondents by country of origin

Country	**Number of respondents**	**Weighted Percentage (%)**
France	12	22.64
Germany	7	13.21
Belgium	5	9.43
USA	5	9.43
Italy	4	7.55
Switzerland	3	5.66
Austria	2	3.77
Netherlands	2	3.77
Czech Republic	1	1.89
Denmark	1	1.89
Estonia	1	1.89
Finland	1	1.89
Norway	1	1.89
Spain	1	1.89
Sweden	1	1.89
UK	1	1.89
N/A	5	9.43
Total	**53**	**100**

During the planning phase of the research, the author assumed that the largest number of all feedback would be from two types of stakeholders: public and private sector organizations of EU Member States. In contrast, the second round of the data analysis revealed that the third sector organizations, EU citizens, and Non-EU organizations actively participated in the consultation. Therefore, the data was split into three groups of stakeholders: public sector, private sector, and others (Appendixes 3 – 5). The following subsections focus on the analysis results of those groups of stakeholders.

5.1 Expectations of the private sector representatives towards eIDAS regulation

The third-round task was to find a generalisation and central themes in each group of stakeholders. The first group of public consultation participants included private sector organisations. This group of participants was thematically analysed to find a generalisation and main themes, patterns, and probable explanations of the challenges and triggers of eIDAS implementation. Altogether, the private sector was represented by 31 respondents from EU Member States (22 responses), non-EU countries (8 responses), and one respondent who preferred to stay anonymous. Further, the statistical data illustrates that large, medium, small, and micro-companies were represented during the feedback collection (Figure 4. Private sector respondents' statistics).



Private sector respondents (31)

EU (22):

France	7
Belgium	5
Germany	5
Austria	2
Denmark	1
Netherlands	1
Sweden	1

Non-EU (8):

USA	4
Switzerland	2
Norway	1
UK	1

N/A (1)

Companies by size:

Large	7
Medium	4
Small	5
Micro	5
N/A	1

Companies by size:

Large	2
Micro	6

Large (250 or more)
Medium (50 to 249 employees)
Small (10 to 49 employees)
Micro (1 to 9 employees)

Figure 4. Private sector respondents' statistics

Business organisations from seven EU countries out of 27 directly participated in the public consultation and sent their feedback. The largest number of responses came from France (7), German and Belgium organisations sent five responses each. Concurrently, it is worth mentioning that business association represented the interests of certain domain companies from a range of countries. Large companies (250 employees and more) constituted 33% of all respondents from EU countries. Small (10 to 49 employees) and micro (1 to 9 employees) organisations contributed equally with a 24% participation rate of all EU companies. Medium companies with 50 to 249 employees amounted to 19% of all respondents from EU countries (Figure 5.).

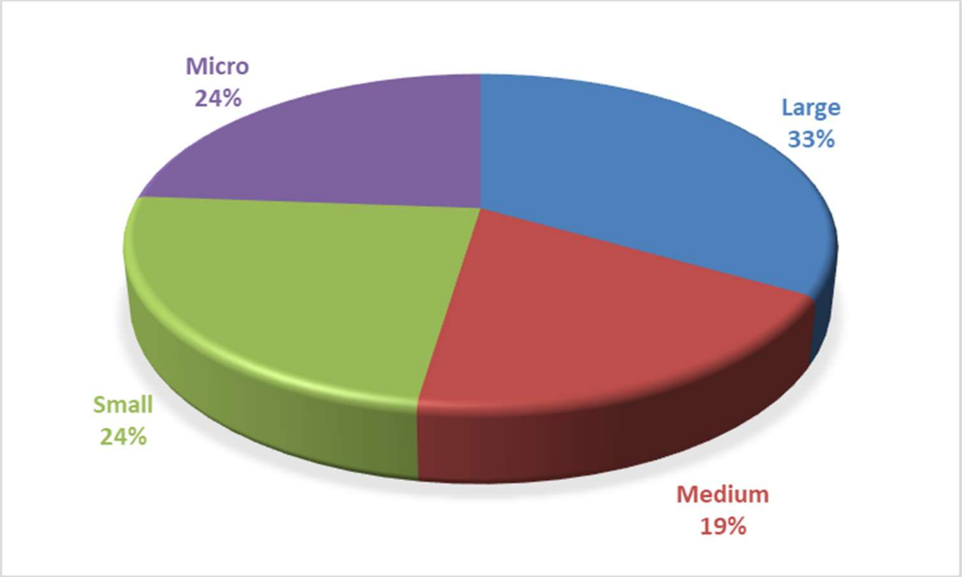


Figure 5. Private sector respondents from EU by size

All participants from the private sector can be split into two groups: separate companies and various business associations. The latter represented interests of different business organizations from finance (2), Internet and IT services (2), identification and trust services (2), insurance (1), postal services (1), and legal affairs (1) domains. Separate companies were from the identification and trust services area (6), telecommunication (3), IT services (2), biometrics technologies (1) and finance (1) domains (Figure 6. Private sector respondents from EU by the sector of the economy).

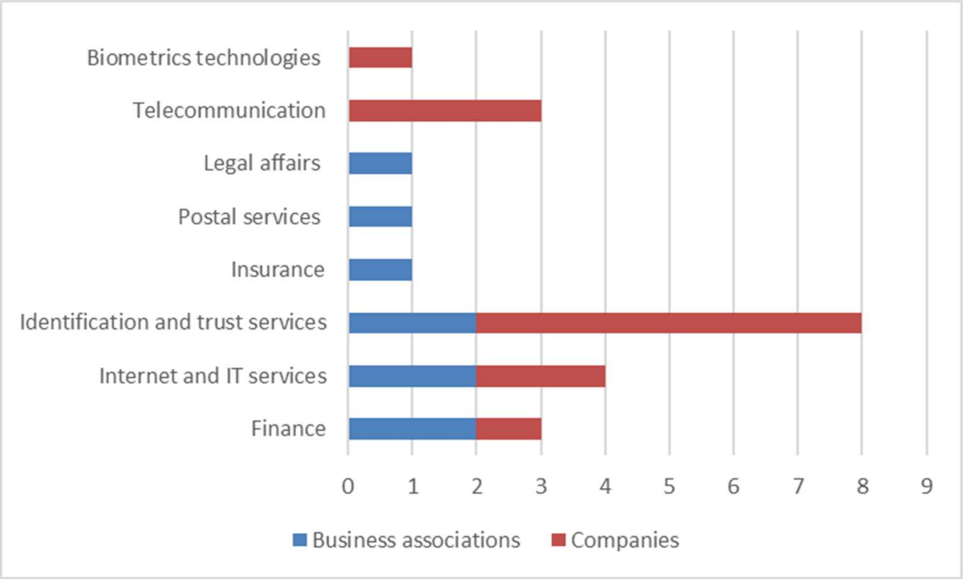


Figure 6. Private sector respondents from EU by the sector of the economy

Among non-EU business, organisations were mainly business associations (5), individual companies (2), and independent domain experts (1) from finance, insurance, software development, cybersecurity, and digital identity domains.

The thematic analysis of the second group of stakeholders illustrated that respondents from the private sector emphasised six groups of challenges in the eIDAS implementation process (

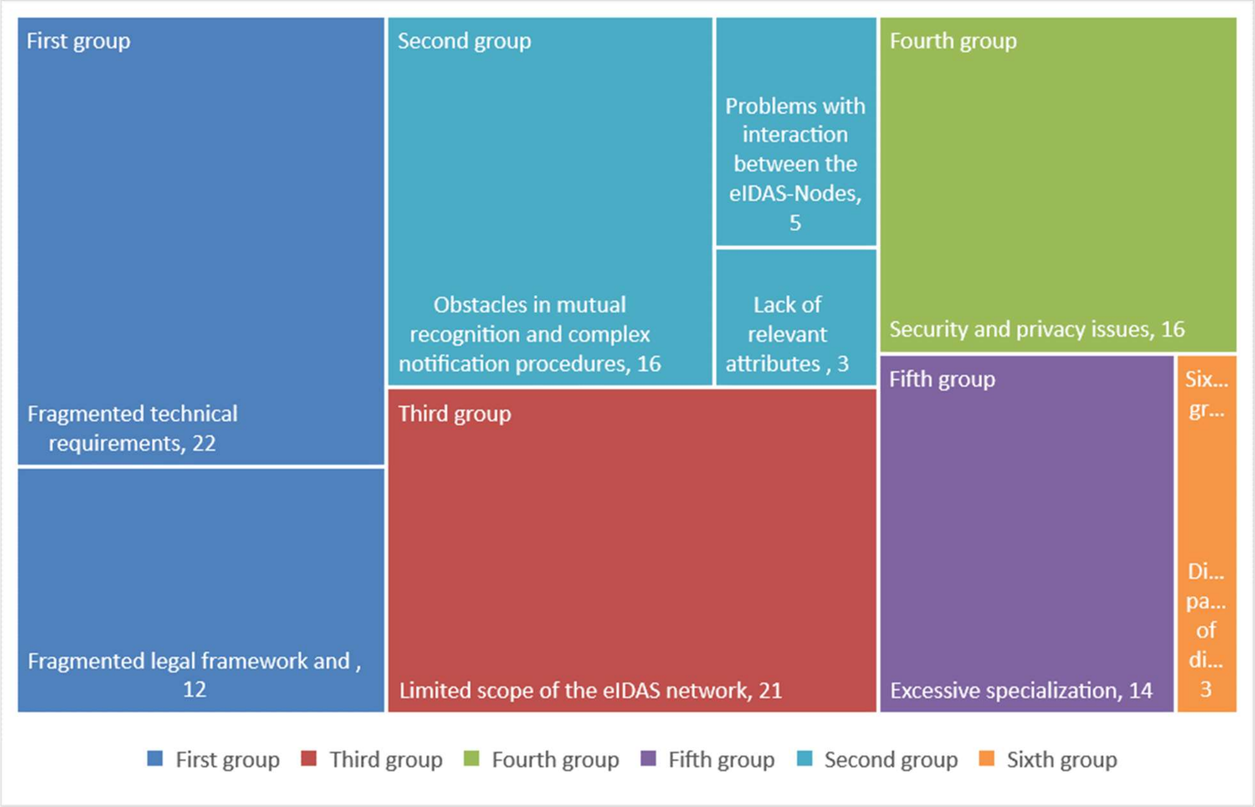


Figure 7. Thematic analysis results of the private sector respondents). This includes the fragmented legal framework and technical requirements, obstacles in mutual recognition and the interaction between the eIDAS-Nodes, the limited scope of the eIDAS network, security and privacy issues, excessive specialisation, and a different pace of digitalisation of the Member States.

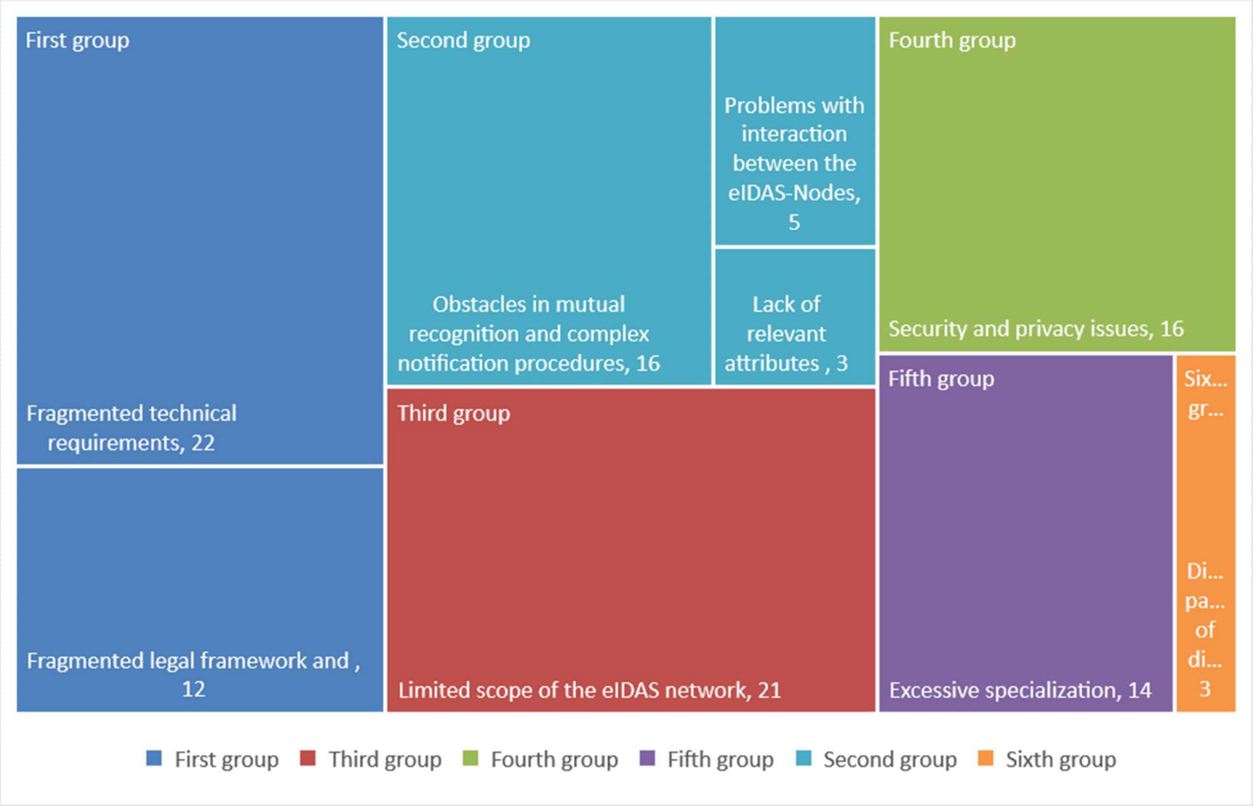


Figure 7. Thematic analysis results of the private sector respondents

The most mentioned problems were connected to fragmentations in the legal framework (12 times) and technical requirements (22 times). Since these two themes are intertwined and difficult to split, they can be considered one group. In the respondents' opinion, the legal framework needs to be more harmonised on the EU level because the national rules of the Member States stay fragmented and undeveloped. Such fragmentation leads to "*a high level of uncertainty for businesses and effectively blocks consumers in some Member States*". Besides the fragmented legislation, "*the technology, eID devices and protocols differ from member state to member state*". There is also *"a lack of common technical standards for digital identity matters"*. For instance, *"the eIDAS does not establish certifiable standards for all digital identity providers"*. The topic of remote identity proofing and its' lack of harmonization is the most mentioned in this group (11 times).

Approximately the same number of respondents from the private sector see obstacles in mutual recognition and eID schemes notification procedures (16 mentions), with the interaction between the eIDAS-Nodes (5) and in lack of relevant attributes (3). The category related to mutual recognition and eID schemes notification procedures includes the complexity of the notification process, incompatible requirements between policies, different interpretations of some articles of the regulation by national authorities. For instance, *"National governments interpretations of the Regulation has complicated the validity and recognition of the electronic signatures between the Member States"*. Representatives from the non-EU countries would like the EU to collaborate on the international level in the eID schemes mutual recognition. They find it *"important that the national e-ID systems should be made easily interoperable not only among EU member states but also with relevant third countries and non-EU financial centres"*.

Moreover, two mentions were regarding lack of advisory institution on the EU level that is *"advisory/administrative body to support the industry by implementing eIDAS"*. Besides, national *"supervisory bodies have no legal enforcing authority"*; therefore, *"a set of baselines of auditing rules and a baselines audit plan for each trust service"* needs to be created. In addition, two mentions were about the management of emergencies topic, which, for instance, needs to include *"Backup eID schemes"* for emergencies. There is also a need to amend the interaction between the eIDAS-Nodes (5 mentions): identity matching is problematic as *"some Member states do not have persistent identifiers"*, *"no access requirements to exchange data between two eIDAS services"*. Further, the lack of relevant attributes for several services was mentioned three times. For example, it is necessary to harmonize attribute definitions and *"enlarge the data set defining natural and legal person with supplemental optional attributes"*.

Another group of obstacles, in the opinion of the private sector respondents, relates to the limited scope of the eIDAS network, lack of demand and use cases, which is mentioned 21 times. *"The current eIDAS framework is restricted to specific use-cases and is not a good fit for many solutions providing digital identity verification, particularly in the private sector."* Since *"the number of cross-border consumer-to-government (C2G) use cases is small relative to the number of consumer-to-business (C2B)",* the framework could be extended to the private sector. For example, *"Private service providers, including online platforms, could integrate with the public eID systems to confirm their users' legal identity."* Moreover, some respondents propose to *"encompass increased* *recognition of private sector identity providers"*. Furthermore, more attention should be drawn to user experience and consumer preferences, including authentication processes.

From the security and privacy aspects (16), respondents argued there is a need for a *"uniform definition of the level of assurance of the identification and authentication procedures and their applicability"*. Currently, there is a deficit of clarity about the levels of assurance and *"too much space for interpretation"*. Overall, the issue with the level of assurance was mentioned nine times. Some representatives suggested that the "*eIDAS regulation should be harmonized with the EU Cybersecurity Act"* and rely on GDPR.

The 14 respondents from the private sector argued that some eIDAS norms are excessively specialized and, in some countries, local regulations are *"restrictive and technology-specific"*. Consequently, the stakeholders warned that excessive regulation might lead to "rapid regulatory obsolescence" and restriction of innovation. For instance, some companies are *"unable to certify under eIDAS, (because) innovative digital identity verification solutions are prohibited from entering some markets"*. Therefore, they propose that eIDAS should remain *"technologically neutral"*. Further, *"any proposed revisions must take into account the dynamic and evolving nature of the digital economy and the infrastructure."* For example, it is offered to include other technical solutions besides SAML. *"Important not to commit to unilateral technical solutions in advance (e.g., SAML or blockchain); to endorse the OpenID Connect Standard besides SAML"*. Among other obstacles, the different pace of digitization across the EU was mentioned three times, for instance, *"not all Member States offer eIDs"*.

Regarding EC options for further eIDAS framework development (1. revise and slightly update the current regulation, 2. extend the effect of eIDAS to the private sector, 3. launch a European Digital Identity (EUid) or combine these three solutions), the preferences of private sector participants were split mainly between various combinations. Besides, 11 respondents, which constitutes 36% of all private-sector respondents, did not choose any option or combination of options (Figure 8).

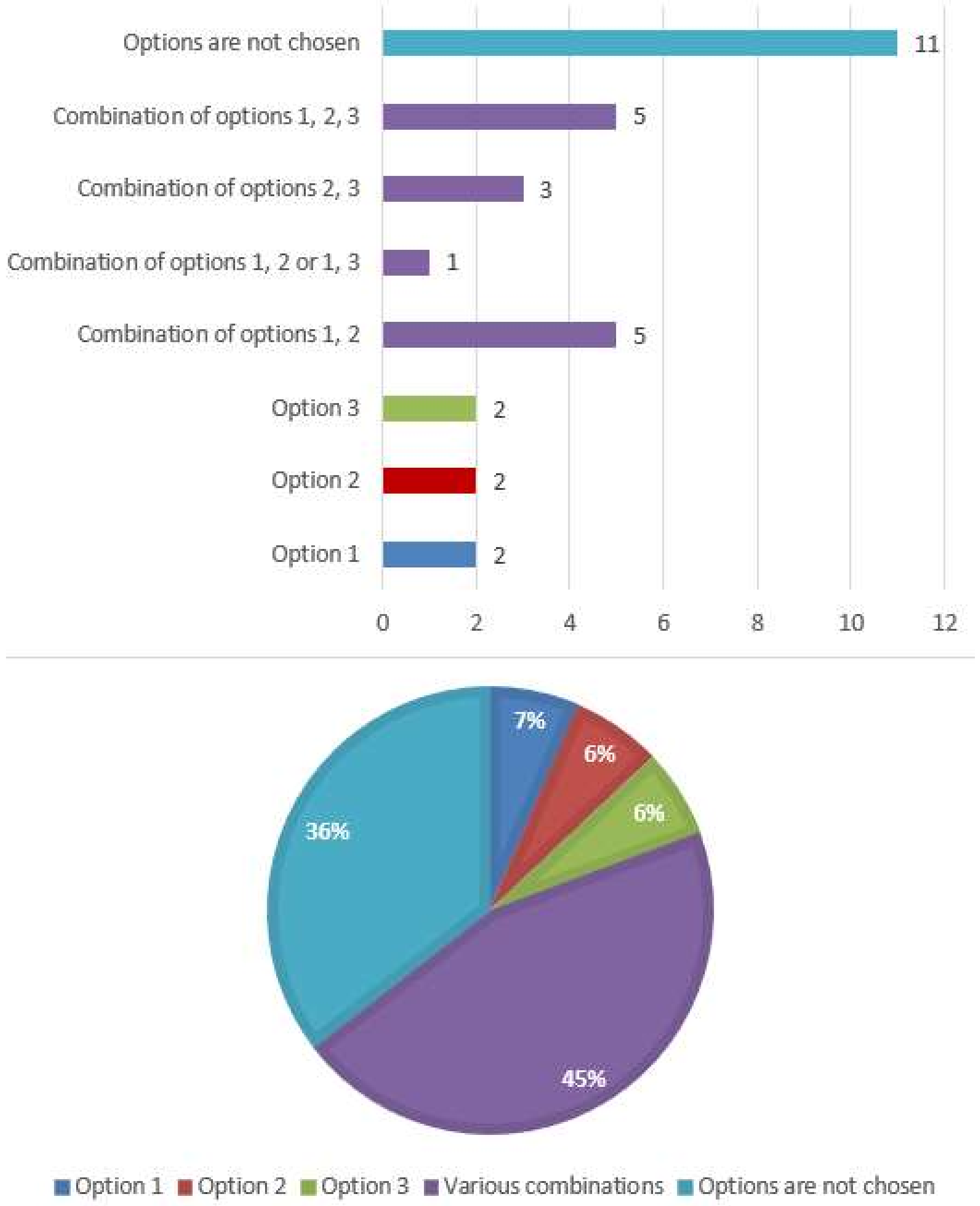


Figure 8. Private sector respondents' preferences

Overall, combinations of option '1' and option '2' and combinations of options 1, 2, 3 were equally popular. The following subsection will elaborate on the third group respondents' preferences in terms of eIDAS development.

5.2 Expectations of the EU Member States public sector organizations towards eIDAS regulation

Among the respondents that presented their feedback on the eIDAS regulation were seven representatives from the public sector organizations: three from the national level, one from local, two from public academic institutions, and one from the postal service provider. Two of them represented France organizations, and others were from Spain, Italy, Estonia, the Netherlands, and Finland. It would be better to explore the academic institutions' feedback separately, yet the small number of responses (two) does not allow generalizations. Therefore, public sector stakeholders' expectations also include an opinion of the research institutions.

Overall, the respondents from the public sector support the idea of eIDAS, considering it as "*a fundamental*", "*valuable concept that definitely strengthens the EU digital single market*". However, at the same time, they notice that it is an "*incomplete basis of legal experience (concerning) electronic agency institutions, especially from the perspective of the private sector*" and "*its potential remains still underexploited*". Consequently, they indicate ensuing challenges such as: "*different practices or interpretation*" of eIDAS, insufficient regulation, or inadequate digital literacy of the population. For instance,

"*Although the electronic signature fully responds to the principle of functional equivalence, the eIDAS Regulation only establishes legal effects with respect to qualified electronic signatures, leaving it to the Member States to stipulate the legal effects of the remaining electronic signatures. This approach is to be criticized as (it) affects negatively the possibility of using nonqualified electronic signatures based on the autonomy of the will of the parties.*"

"*We have seen the shift towards a more attribute-based approach in the current revision, but we have not seen such a clear shift towards decentralized architectures, where the storage of attributes is under the direct (physical) control of users and is not under (the) control of intermediate parties (who can then monitor who authenticates where (and) with which attributes). In short, we believe the eIDAS approach would benefit from privacy by design via decentralized electronic identities.*"

The most mentioned problems are related to the lack of standardization and control (is mentioned in 4 responses). Among the propositions to improve the eIDAS from the respondents' point of view are the following measures:

- to cover transactions between private parties,
- standardize the peer-review procedure,
- specify the minimum criteria relating to remote identification,
- determine the identification of devices and the Internet of Things procedures,
- organize training for citizens.

"For the proper development of the Digital Single Market, Member States should be required to ensure that the means of electronic identification which they notify can also be used for transactions between private parties."

"This situation could be corrected by regulating electronic identification as a trust service. The revised version of the eIDAS Regulation should create a legal rule allowing natural and legal persons to use a qualified electronic signature or seal certificate where the law imposes the requirement to identify their selves."

Some respondents argue that the trust services list should be further expanded:

"The eIDAS Regulation has not exhausted, by express decision of the legislator, the list of institutions used for the accreditation of electronic agency, allowing the Member States to maintain or create other trust services... But this is a relevant problem for a Digital Single Market as it entails a significant level of heterogeneity and fragmentation that can hinder its achievement. Various legislations have already regulated the electronic archive as an institution based on the corresponding trust service, ... It would be convenient for these institutions to join the harmonized regulation at the Union level. As long as this does not happen, important differences remain in the management of documents."

Alternatively, in others' opinion: "*The introduction of digital identity trusted services, other than the eIDs already implemented under the eIDAS Regulation, should not be pursued. As previously noted, if this were to happen it could undermine the massive* *efforts, organizational and economic, put in place by the Member States that have already developed notified digital identity systems."*

At the same time, one reply directs attention to the lack of technological variations of the qualification mechanism, as in some cases, it is "*excessively specific*", which may undermine "*the standards of technological neutrality*" and perspectives of "*emerging electronic identity and trust services technologies.*" It is worth mentioning that the technological neutrality issue was also stressed by the earlier research (Veerpalu et al., 2020). Equally important this matter is apparently to be for one respondent as it is proposed: *"the qualification should be more abstract, so that any electronic signatures, electronic seals or other institutions of accreditation of electronic performance that are not based on the use of cryptographic keys (such as the handwritten signature captured electronically), can be qualified. ... This is particularly relevant for emerging electronic identity and trust services technologies, such as Distributed Ledger Technologies (e.g. blockchains) supporting the so-called Self-Sovereign Identities, currently being explored by the European Commission in the EBSI project."*

The three options of further eIDAS development proposed by the EC, i.e. 1) revise and slightly update the current regulation, 2) extend the effect of eIDAS to the private sector, 3) launch a European Digital Identity (EUid) or combine these three solutions, were discussed in the feedback too. Opinions were split between the first, second, and combined option. Those favouring the first option are concerned about additional financial costs and organizational changes of the already existing systems, which the second and third solutions might cause. Only one respondent entirely supported the first option. *"The first option, properly integrated, seems to be the only one effectively pursuable."*

"The others, while presenting points of value, might introduce some critical elements, with potential economical and organizational impacts on the digital identity models currently in place."

The second option is more attractive to those, who value further expansion of eIDAS, especially to the private sector *"the most valuable scenario is option 2, as it leverages the strong electronic identification capabilities of Member States while creating wider markets for private providers."* One respondent supported this option.

The respondents of the public sector do not much support the third option due to financial considerations:

"*The introduction of a new European digital identity system (EUid) complementary to eIDAS for citizens' access to public and private online services does not seem to bring particular advantages; on the contrary, it could jeopardize the investments made to date. In fact, the intervention might appear as a disincentive with respect to what has been developed up to now and to the schemes currently notified and with a growing adoption rate throughout Europe.*"

"According to the provided documentation, option 3 would result in setting up a parallel scheme to the already existing eID schemes. Therefore, this option adds complexity to the eIDAS ecosystem and presumes additional funding. Therefore, we recommend conducting a cost-benefit analysis regarding this option, in particular, because of the use of the EUid is planned to be voluntary."

"Common ID cross member states would make it easier to manage patient information from other member states and people travelling between member states… However, current ID is implemented in so many systems already that changing the format or content of the ID has been estimated to cause several hundreds of millions of costs and requiring several years to implement."

However, one respondent pointed out that the third option is favourable for the identities of legal persons. Meanwhile, another respondent entirely approved the proposal of EC "to make notification of national schemes under eIDAS mandatory" (Inception impact assessment, 2020):

"*The introduction of a mandatory notification of at least one eID scheme for each Member State (with the mutual recognition of notified systems) would instead have significant benefits.*"

Alternative options or combinations of them are supported by two respondents, for instance:

"By combining option 1 and option 2, it is possible to significantly improve the current situation and make eIDAS more unambiguous and transparent."

"A solution that takes into account all three options might be the most ideal. "

Other respondents from the public sector were more concerned about principles of electronic identities than choosing between proposed options. People-centred approach with privacy by design, decentralized architecture, data minimization were drawn to the attention three times. Remote identification, face recognition were mentioned by two respondents.

Overall, it is difficult to generalize in the case of public sector stakeholders as not many public organizations and countries were represented. The respondents were concerned about standardization that needs to be specified or improved on their opinion. Moreover, privacy and a people-centred approach were important for others. Furthermore, the respondents had different opinions about proposed options on the eIDAS development. The following section provides research results related to the third sector and other participant's opinion on the further eIDAS development issues.

5.3 Expectations of the third sector organizations, EU citizens, and other stakeholders

The third group of respondents included 15 participants: 10 from the EU Member States, two from non-EU countries (the USA and Switzerland), and three respondents with unavailable data (Figure 9. Third group respondents' statistics). The most considerable number of responses in this group of participants came from France (4), then followed respondents from Italy with three replies, Germany with 2, and the Czech Republic with 1. Among the participant in this group were five NGOs from the identification, trust services and research domains, five EU citizens, one council of notaries, and four preferred to remain anonymous.

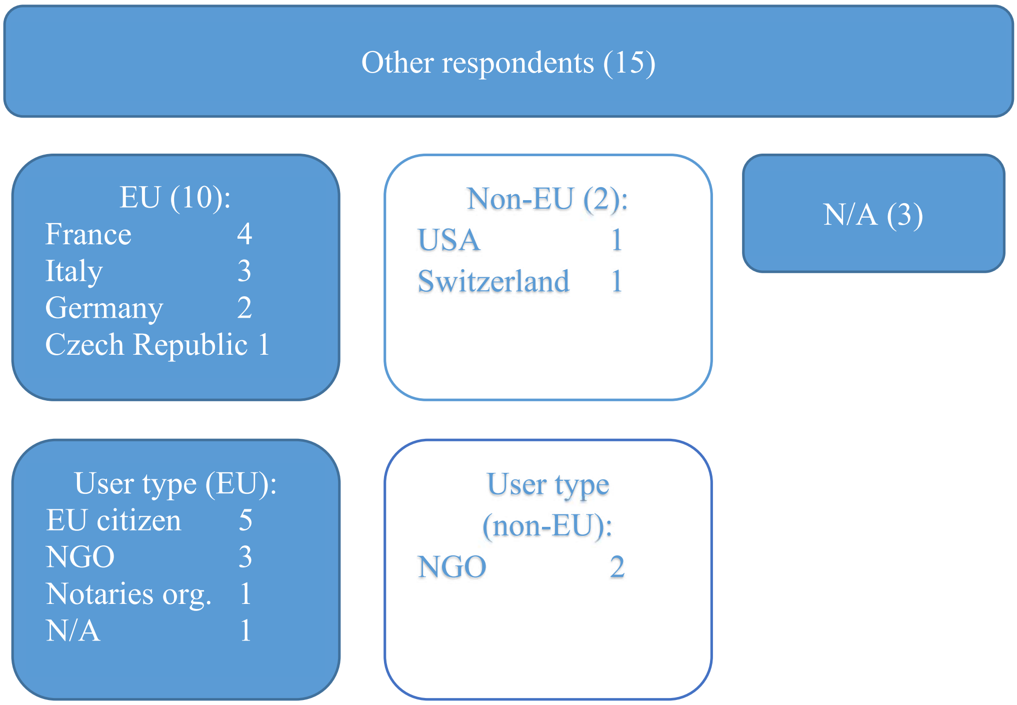


Figure 9. Third group respondents' statistics

The thematic analysis of the third group of stakeholders depicted that mainly four groups of challenges in the eIDAS implementation process that need improvement were mentioned (Figure 10. Thematic analysis results of the third group of respondents). This includes the first group with fragmented technical requirements and legal framework, the second group with e-IDs mutual recognition and lack of relevant attributes, the third group about the limited scope of use cases, and security and privacy issues. Challenges from the last two groups were mentioned once in each case.

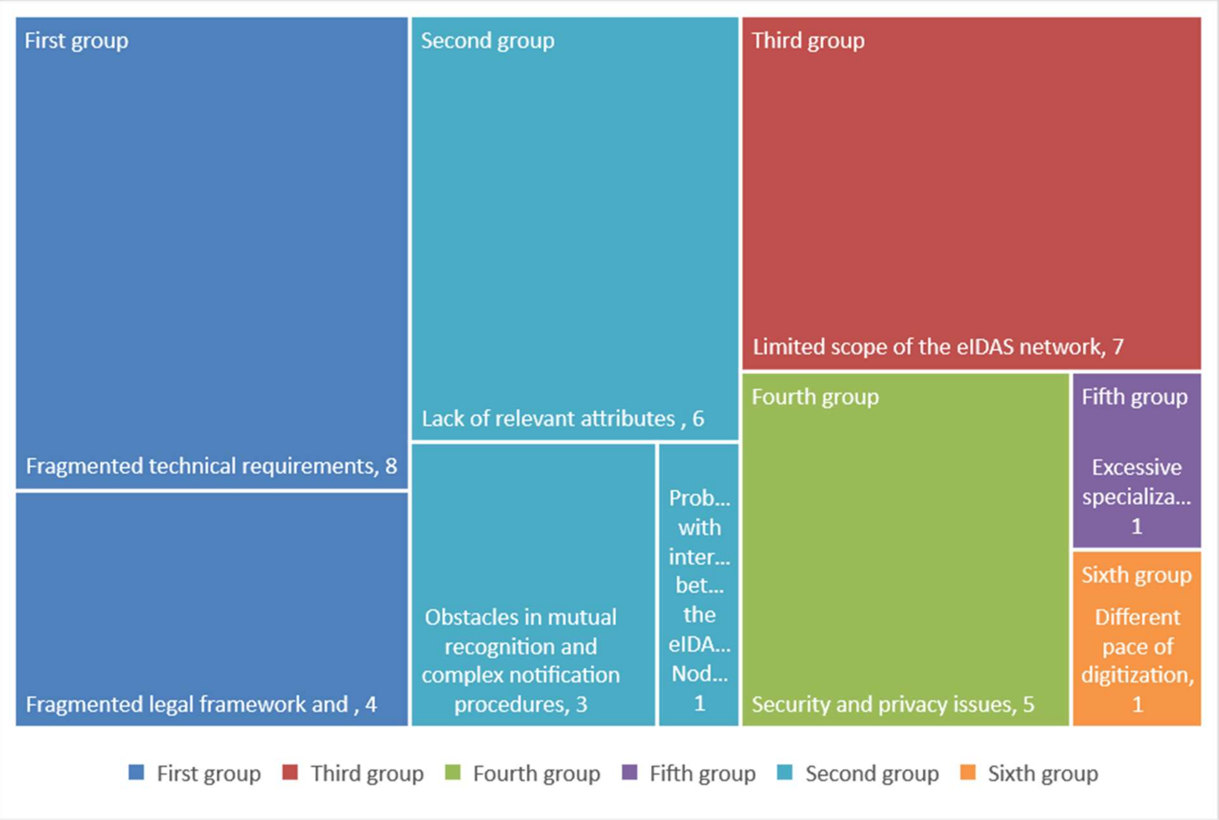


Figure 10. Thematic analysis results of the third group of respondents

The most mentioned issue in the third group of stakeholders was technical requirements fragmentation (8). For instance, one respondent stated that *"The European Commission should also propose measures to strengthen the standardization of quality certificates in order to make it easier to qualify in the different Member States and to read certificates"*. Overall, more strategic directions are needed for leveraging the benefits for the end-users and the system. As a solution, among other suggestions, it was recommended: *"to call the European Standard Organizations to complete the current set of standards that are referenced into the eIDAS"*. However, the EC should take care and *"not to overregulate"* and let *"trending technologies"*, such as biometric recognition, be leveraged.

The limited scope of the eIDAS framework was mentioned seven times. As a solution, it was proposed to *"introducing market forces"* and *"stimulate the market for tools for providing trust services",* thus boosting creativity and competition in Europe. Overall, *"to consider extending its recognition to the private sector"*, to promote *"the use of trusted identities for all Europeans"*, and *"to create new "trust services"*. However, some respondents argue that *"application of the eID scheme to the private sector (should be) provided for a specific access fee defined at the national level"*. Some non-EU participants from this group reminded to consider the cases where EU citizens need to use electronic identities outside of the EU and extend interoperability to the international partners.

Security and privacy topics are essential for this group of stakeholders as well (5 mentions). For instance, some respondents concerned about private trust service providers, who might not guarantee sufficient security to personal data if there are no specific rules and standards to follow. Therefore, the EC should define *"a model"* and *"specific obligations for private service providers"* and leverage *"the eID scheme to the private sector - starting from the one already implemented for the public sector"*.

Lack of relevant attributes was mentioned six times, while obstacles in mutual recognition – three times. Some respondents believed that *"the notification process at European level shall remain a prerogative"*. Moreover, some of them argue that *"different identifiers (cannot) recognize each other in digital platforms"*. It was suggested to *"consider harmonisation of legal entity datasets"* and harmonise the identities of professionals. As a solution, it was suggested using Legal Entity Identifier (LEI), linking "*persons and companies and devices and companies",* thus increasing "*interoperability of the eIDAS framework, making cross-border electronic transactions more efficient and secure"*. Further, it was mentioned that *"most commercial identity providers provide a mixture of attributes maintained according to different trust frameworks and at different trust levels… for the same identity"*. Therefore, it was proposed to utilise such use cases as well.

Almost half of the respondents of this group preferred to notify the EC about their concerns on further eIDAS framework development and not to choose between the proposed option in the Inception impact assessment (Figure 11. Third group respondents' preferences). Opinions of other participant were split between the first (3), second options (3), and combination of all three variants that were proposed (2).

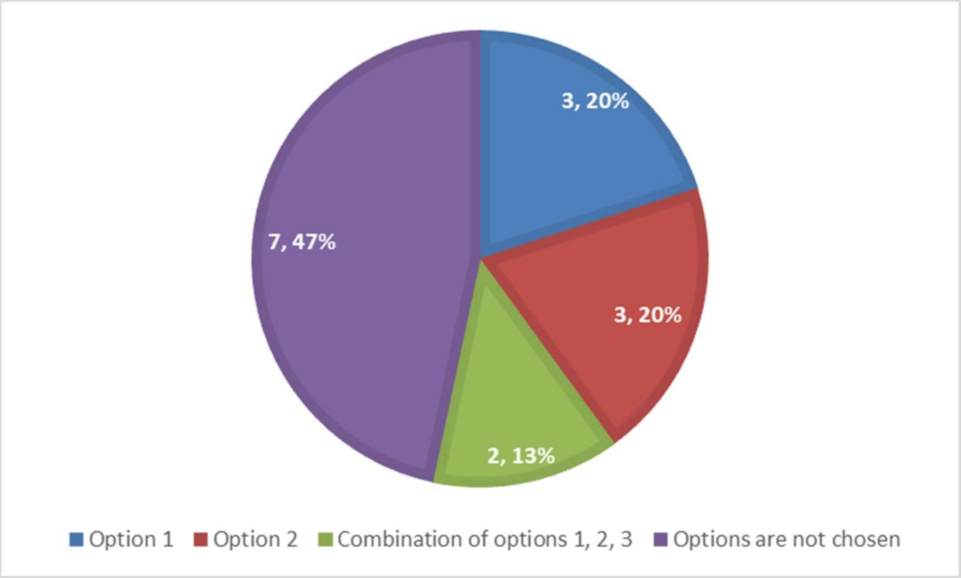


Figure 11. Third group respondents' preferences

Common challenges from all three respondents' groups will be provided in the following subsection.

5.4 Common challenges and expectations from Stakeholder's Perspective

Based on the thematic analysis of all three groups of stakeholders, similar problems and core issues for all participants were defined. These issues include fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure, and excessive specialization (Figure 12. Thematic analysis results of the fourth round). The most mentioned problem by the participants that need to be improved is related to fragmented technical requirements (33). The limited scope of eIDAS and use cases had almost the same amount of attention (31 mentions). Security and privacy aspects also need a significant amount of attention (25 mentions) on respondents' opinion. The problems related to the notification procedure with 20 mentions, a fragmented legal framework with 20, and excessive specialization with 16 references require improvements and clarifications by the opinion of all participants.

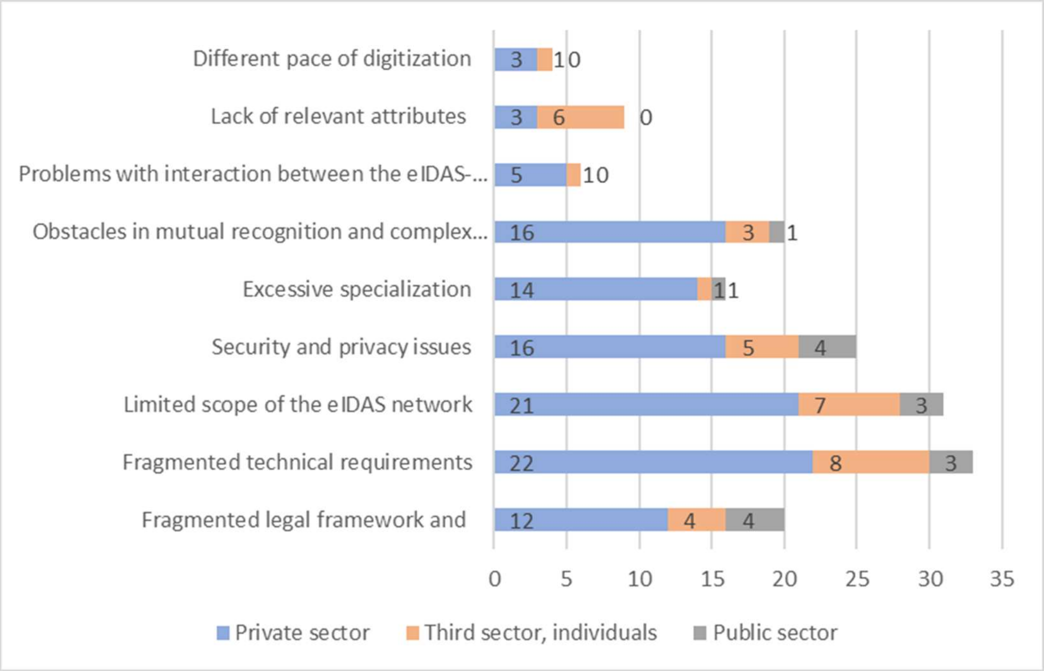


Figure 12. Thematic analysis results of the fourth round

Regarding three variants of further eIDAS development proposed by the EC, i.e., 1) revise and slightly update the current regulation, 2) extend the effect of eIDAS to the private sector, 3) launch a European Digital Identity (EUid) or combine these three solutions, 34% of all respondents chose various combinations of options (Figure 13. Respondents' preferences). The most popular among combinations is an incremental approach that requires implementing the options step by step, starting from the first, then moving to the next option. However, the implementation of two first variants (1 plus second option) is also quite popular. The first variant, which implies slight revision and supplement of the framework, is preferred by 11% of all participants. Those who chose this variant informed that they do not wish for significant changes in the eIDAS framework. Equally supported is the second option (11%) that presumes major revision of the legislation, extension of the scope to the private sector, and creation of new trust services. At the same time, 40% of all respondents concentrated on the points which need revision, adoption, or other improvements and did not clearly state any option from the proposed three.

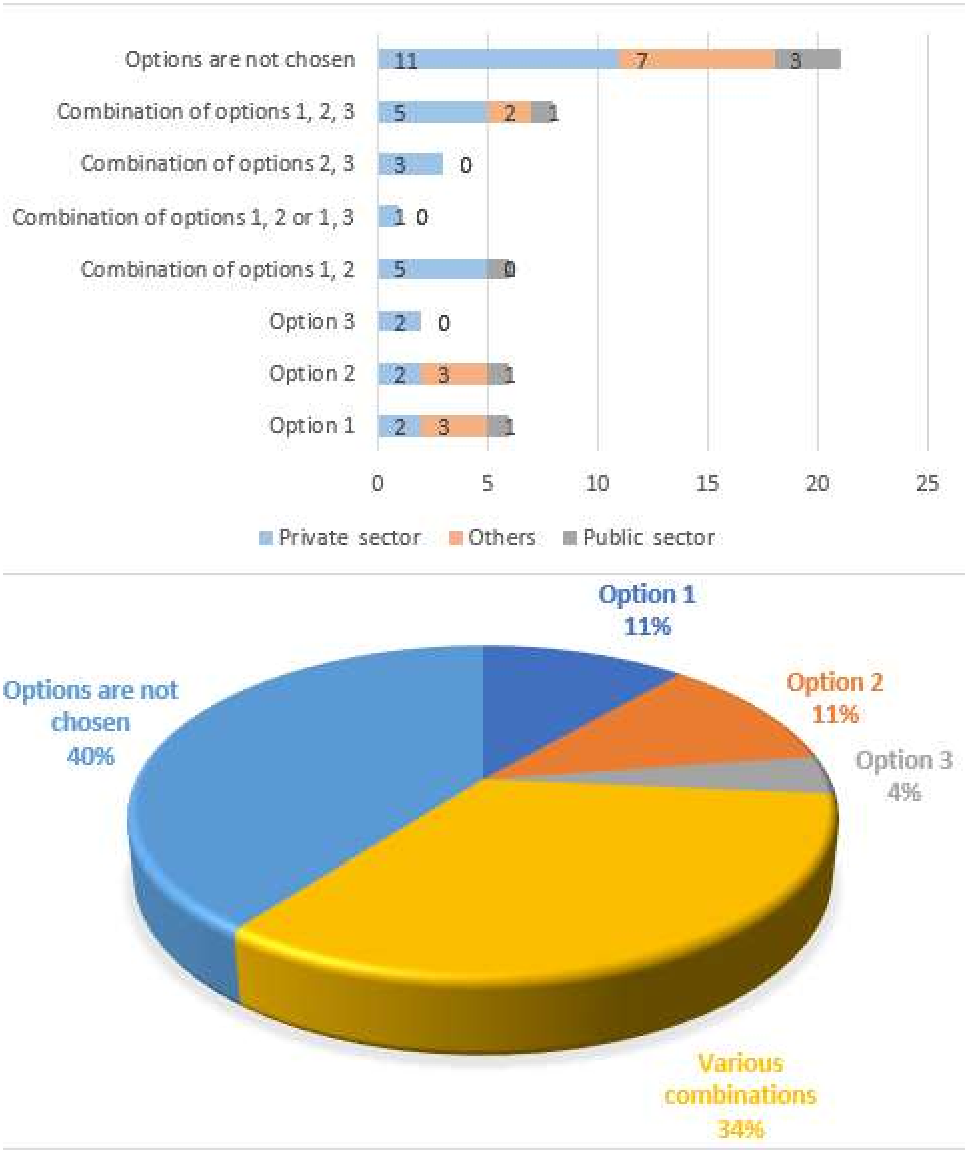


Figure 13. Respondents' preferences

The following section provides further discussion and recommendations on eIDAS development.

6 Discussion and recommendations for the further eIDAS review process based on the identified expectations

The overview of the national eID systems and the eIDAS implementation status illustrates differences between the countries, confirming the previous research that some countries are more successful in the eIDAS implementation. Based on the research results, it is possible to conclude that the respondents see various challenges in the eIDAS implementation, and many of them are similar. Among mentioned obstacles are fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure, and excessive specialization. Those perceived shortcomings correspond with the previous research results that indicated “compliance issues”, “interpretation problems”, “different practices in member states”, and “representation of legal person challenges” (Lips et al., 2020). Stakeholders, similar to researchers, propose to widen the scope of the technological solution and discuss privacy issues.

Despite the similarities in perceived challenges, participants have different expectations for the eIDAS further development. The short list of proposed recommendation represents the variety of the stakeholders’ opinions (Appendix 9). Some prefer slight changes and a very cautious approach due to the possible additional costs or probable increase in competition. Alternatively, others welcome more profound and brisk alterations and an increase in competition in the trust services domain to reach higher efficiency and security. Some expect an incremental, gradual approach with the involvement of specialists and stakeholders to guard the interests of all players. Moreover, non-EU stakeholders wish to be engaged in the process and reach global interoperability to lower costs and administrative burden. Social media domain representatives seek to protect their interests and wish their customers to continue using their identification and authentication services.

Interestingly, that non-EU companies actively participated in the public consultation. Meanwhile, EU public sector organizations did not express the same interest in the event. The private sector view was stronger presented. Further, it is possible to notice that France was very much engaged in the consultation with the most significant share of all participants. The probable explanation of such interest was that France was preparing to pre-notify its’ eID schemes under eIDAS at that time, which resonated through a high participation rate in the consultation. The low number of respondents from the public sector and citizens’ representatives limit the possibilities to generalize the research results. Moreover, the results reflect only opinions of those, who provided their feedback on the EC proposal. Therefore, there might be other solutions to master mentioned challenges and improve eIDAS implementation.

7 Summary

The eIDAS revision is a part of the EU strategy because the EU Digital Single Market largely depends on its enablers: eIDs and electronic Trust Services. Therefore, its' revision requires a thorough evaluation involving all stakeholders to avoid further obstacles. Their feedback on implementation hurdles and expectations for the eIDAS further development needs to be thoroughly analysed to become a base for future improvements in the framework. The study's primary purpose was to fill the gap in research, providing additional knowledge in understanding the obstacles and triggers of the EU digital identity implementations and giving recommendations in the further development of the eIDAS.

The overview of the national eID systems illustrated that the eID systems vary significantly within the boundaries of the EU. Some countries had been providing their citizens with electronic identifications for years, while others had just started working on the solutions. Since the eIDAS adoption, the Member States gradually started notifying their eID schemes. Further, the research explored the stakeholders' feedback on the EC proposal from 23 July 2020 (Inception impact assessment, 2020).

The research results suggest that the respondents see various challenges in the eIDAS implementation, and many are similar. Among mentioned obstacles are fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure, and excessive specialisation. Despite the similarities in perceived challenges, participants have different expectations for the eIDAS further development.

Ultimately, the issue of the eIDAS revision is very complex, involves many stakeholders, and require thorough evaluation and negotiations. As literature suggested, the difficulties in eIDAS implementation might be caused by the complexity of the eID concept, which encompasses more than outlined by the EU frameworks. Therefore, the revision requires additional research of the stakeholders' expectations, including public sector organisations, citizens, and experts.

References

[1] Administrative Modernization Agency. (2021a). *Autenticacao.gov. Outros meios de autenticação*. https://www.autenticacao.gov.pt/web/guest/outros-meios/outros-meios-de-autenticacao

[2] Administrative Modernization Agency. (2021b). *Autenticacao.gov. Sobre o Cartão de Cidadão*. https://www.autenticacao.gov.pt/o-cartao-de-cidadao#_ga=2.228245593.574981983.1616996747-642046205.1616996747

[3] Administrative Modernization Agency. (2021c). *Eportugal.gov.pt. Login to the portal*. https://eportugal.gov.pt/en/entrar

[4] Agency for Digital Italy. (2021). *SPID. Public Digital Identity System*. https://www.spid.gov.it/richiedi-spid

[5] Agency for Digitisation. (2019). *Notification form for electronic identity scheme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Denmark?preview=/129105932/200867933/NOTIFICATION%20FORM%20FOR%20ELECTRONIC%20IDENTITY%20SCHEME%20UNDER%20ARTICLE%209-1%20-%20version%20final%20(2).pdf

[6] Agency for Digitisation. (2021). *Next generation NemID*. https://en.digst.dk/digitisation/eid/next-generation-nemid/

[7] Al-Hujran, O., Al-dalahmeh, M., & Aloudat, A. (2011). The Role of National Culture on Citizen Adoption of eGovernment Services: An Empirical Study. *Electronic Journal of E-Government*, *9*(2).

[8] Al-Khouri, A. M. (2014). Digital identity: Transforming GCC economies. *Innovation*, *16*(2), 184–194. https://doi.org/10.1080/14479338.2014.11081981

[9] Alonso, Á., Pozo, A., Gordillo, A., López-Pernas, S., Munoz-Arcentales, A., Marco, L., & Barra, E. (2020). Enhancing University Services by Extending the eIDAS European Specification with Academic Attributes. *Sustainability (Basel, Switzerland)*, *12*(3), 770.

[10] A-trust. (2021). *Handy-signatur. Id-Austria.* https://www.a-trust.at/en/handy-signatur/id-austria/

[11] Authority for the Digitalisation of Romania. (2021a). *Adr.gov.ro. Platforma Software Centralizată pentru Identificare Digitală—PSCID*. https://www.adr.gov.ro/proiecte-in-implementare/platforma-software-centralizata-pentru-identificare-digitala-pscid/

[12] Authority for the Digitalisation of Romania. (2021b). *Ghiseul.ro—Sistemul National Electronic de Plata Online. Solicitare date de acces*. https://www.ghiseul.ro/ghiseul/public/credentiale

[13] Backhouse, J. (2006). Interoperability of identity and identity management systems. *Datenschutz Und Datensicherheit - DuD*, *30*(9), 568–570. https://doi.org/10.1007/s11623-006-0145-y

[14] Berbecaru, D., Lioy, A., & Cameroni, C. (2019). Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information (Basel)*, *10*(6), 210.

[15] Buccafurri, F., Lax, G., Russo, A., & Zunino, G. (2018). Integrating Digital Identity and Blockchain. In H. Panetto, C. Debruyne, H. A. Proper, C. A. Ardagna, D. Roman, & R. Meersman (Eds.), *On the Move to Meaningful Internet Systems. OTM 2018 Conferences* (pp. 568–585). Springer International Publishing.

[16] Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2021a). *Oesterreich.gv.at. ID Austria. Informationen zum Pilotbetrieb*. https://www.oesterreich.gv.at/themen/dokumente_und_recht/id-austria/pilotbetrieb.html

[17] Bundesministerium für Digitalisierung und Wirtschaftsstandort. (2021b). *Login at 'oesterreich.gv.at'*. https://eid.oesterreich.gv.at/authHandler/auth/start?token=ZXlKaGJHY2lPaUprYVhJaUxDSmxibU1pT2lKQk1USTRSME5OSW4wLi5ZOUtvQURlVFdTdGp1NHpaLlBQTFRRN0hRXzJyenRQRHY5bEdaamlfbTRUdkFieE9zX21ZY092YWFPbElJRHQ1NER1Vm1HOEVOblRyeFQ3QTBnQTA5SlU1bEttS2cyZjg4ZHA4ZGswanVjLVhjdkVrVlA0WXAwOHcuOVlaRklJTUR2TnVVVW5SWHdLR1Nadw%3D%3D

[18] COM/2015/0192 final. (2015). *A Digital Single Market Strategy for Europe*. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[19] COM/2020/67 final. (2020). *Shaping Europe's digital future*. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN

[20] Department of IT Services. (2021a). *Government Gateway Portal (Ariadni).* https://eservices.cyprus.gov.cy/EN/Pages/Home.aspx

[21] Department of IT Services. (2021b). *Web Portal of the Republic of Cyprus*. http://www.cyprus.gov.cy/portal/portal.nsf/citizen_en?OpenForm&access=0&SectionId=citizen&CategoryId=none&SelectionId=home&print=0&lang=en

[22] Departmnt of Social Protection. (2021). *MyGovID. How do I sign up to MyGovID*. https://www.mygovid.ie/en-IE/HowDoISignUp

[23] Digital and Population Data Services Agency. (2021). *Suomi.fi. Information on e-identification. Identification using different identification tokens*. https://www.suomi.fi/instructions-and-support/information-on-eidentification/identification-using-different-identification-tokens

[24] EC. (2019). *European Commission. Shaping Europe's digital future. National eIDs of six countries available for the EU citizens to use cross-border*. https://ec.europa.eu/digital-single-market/en/news/national-eids-six-countries-available-eu-citizens-use-cross-border

[25] EC. (2020a). *European Commission. EU digital ID scheme for online transactions across Europe. Public consultation*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-/public-consultation

[26] EC. (2020b). *European Commission. Published initiatives. EU digital ID scheme for online transactions across Europe*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe

[27] EC. (2021). *European Commission. Internal Market, Industry, Entrepreneurship and SMEs. The European single market. The single digital gateway*. https://ec.europa.eu/growth/single-market/single-digital-gateway_en

[28] eID User Community. (2018). *Republic of Croatia. Notification form for HR electronic identity scheme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Croatia

[29] eID User Community. (2019a). *eID User Community. Overview of pre-notified and notified eID schemes.* https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[30] eID User Community. (2019b). *Estonian eID notification form for electronic identity scheme*. file:///C:/Users/nvino/Downloads/ESTONIAN%20eID%20NOTIFICATION%20FORM%20FOR%20ELECTRONIC%20IDENTITY%20SCHEME%20UNDER%20ARTICLE%209%20OF%20eIDAS%20REGULATION%20v1.1.pdf

[31] eID User Community. (2020a). *Documentation about the SK eID scheme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Slovakia+-+eID+Scheme

[32] eID User Community. (2020b). *Overview of pre-notified and notified eID schemes under eIDAS*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia

[33] eID User Community. (2021a). *Overview of pre-notified and notified eID schemes under eIDAS. France*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/France

[34] eID User Community. (2021b). *Overview of pre-notified and notified eID schemes under eIDAS. Malta*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Malta

[35] EPC. (2010). *European Policy Centre. The Economic Impact of a European Digital Single Market*. EPC. https://www.copenhageneconomics.com/publications/publication/the-economic-impact-of-a-european-digital-single-market

[36] Gerakos, K., Maliappis, M., Costopoulou, C., & Ntaliani, M. (2017). Electronic Authentication for University Transactions Using eIDAS. In S. K. Katsikas & V. Zorkadis (Eds.), *E-Democracy – Privacy-Preserving, Secure, Intelligent E-Government Services* (pp. 187–195). Springer International Publishing.

[37] Government of Spain. (2014). *Clave.gob.es. What is Cl@ve?* https://clave.gob.es/clave_Home/en/clave/queEs.html

[38] Hoikkanen, A., Bacigalupo, M., Lusoli, W., Maghiros, I., & Nikolov, S. (2010). Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies. In E. de Leeuw, S. Fischer-Hübner, & L. Fritsch (Eds.), *Policies and Research in Identity Management* (pp. 41–58). Springer Berlin Heidelberg.

[39] Identity Malta Agency. (2021). *Identity Malta. E-ID Single Sign On Account*. https://identitymalta.com/services/e-id-sso-account/

[40] Inception impact assessment. (2020). *Proposal for a European Digital Identity (EUid) and Revision of the eIDAS Regulation*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=cellar:35274ac3-cd1b-11ea-adf7-01aa75ed71a1

[41] Information Society Development Committee. (2021). *E-Government Gateway. Administrative and public e-services portal. Login*. https://www.epaslaugos.lt/portal/nlogin

[42] Information System Authority. (2021). *Smart-ID. Introduction*. https://www.id.ee/en/article/smart-id/

[43] Joinup platform. (2020a). *Digital Public Administration factsheet 2020. Estonia*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Estonia_vFINAL.pdf

[44] Joinup platform. (2020b). *Digital Public Administration factsheet 2020. Finland*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Finland_vFINAL.pdf

[45] Joinup platform. (2020c). *Digital Public Administration factsheet 2020. France*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_France_vFINAL.pdf

[46] Joinup platform. (2020d). *Digital Public Administration factsheet 2020. Germany*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Germany_vFINAL.pdf

[47] Joinup platform. (2020e). *Digital Public Administration factsheet 2020. Greece*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Greece_vFINAL.pdf

[48] Joinup platform. (2020f). *Digital Public Administration factsheet 2020. Hungary*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Hungary_vFINAL.pdf

[49] Joinup platform. (2020g). *Digital Public Administration Factsheet 2020. Ireland*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Ireland_vFINAL.pdf

[50] Joinup platform. (2020h). *Digital Public Administration Factsheet 2020. Italy*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Italy_vFINAL.pdf

[51] Joinup platform. (2020i). *Digital Public Administration Factsheet 2020. Latvia*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Latvia_vFINAL.pdf

[52] Joinup platform. (2020j). *Digital Public Administration Factsheets. Czech Republic*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_CzechRep_vFINAL.pdf

[53] Joinup platform. (2020k). *Digital Public Administration Factsheets. Denmark*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Denmark_vFINAL.pdf

[54] Joinup platform. (2020l). *The Digital Public Administration factsheets 2020. Austria*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Austria_vFINAL_2.pdf

[55] Joinup platform. (2020m). *The Digital Public Administration factsheets 2020. Bulgaria*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Bulgaria_vFINAL_0.pdf

[56] Joinup platform. (2020n). *The Digital Public Administration factsheets 2020. Cyprus*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Cyprus_vFINAL.pdf

[57] Joinup platform. (2020o). *The Digital Public Administration factsheets 2020. Lithuania*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Lithuania_vFINAL.pdf

[58] Joinup platform. (2020p). *The Digital Public Administration factsheets 2020. Luxembourg*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Luxembourg_vFINAL.pdf

[59] Joinup platform. (2020q). *The Digital Public Administration factsheets 2020. Malta*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Malta_vFINAL.pdf

[60] Joinup platform. (2020r). *The Digital Public Administration factsheets 2020. Poland*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Poland_vFINAL.pdf

[61] Joinup platform. (2020s). *The Digital Public Administration factsheets 2020. Portugal*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Portugal_vFINAL.pdf

[62] Joinup platform. (2020t). *The Digital Public Administration factsheets 2020. Romania*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Romania_vFINAL.pdf

[63] Joinup platform. (2020u). *The Digital Public Administration factsheets 2020. Slovakia*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Slovakia_vFINAL.pdf

[64] Joinup platform. (2020v). *The Digital Public Administration factsheets 2020. Slovenia*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Slovenia_vFINAL_1.pdf

[65] Joinup platform. (2020w). *The Digital Public Administration factsheets 2020. Spain*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Spain_vFINAL_1.pdf

[66] Joinup platform. (2020x). *The Digital Public Administration factsheets 2020. Sweden*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Sweden_vFINAL.pdf

[67] Joinup platform. (2020y). *The Digital Public Administration factsheets 2020. The Netherlands*. https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Netherlands_vFINAL.pdf

[68] Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in digital identity systems: Models, assessment, and user adoption. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9248*, 273–290.

[69] Klobučar, T. (2019). Facilitating Access to Cross-Border Learning Services and Environments with eIDAS. In P. Zaphiris & A. Ioannou (Eds.), *Learning and Collaboration Technologies. Ubiquitous and Virtual Environments for Learning and Collaboration* (pp. 329–342). Springer International Publishing.

[70] Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society*, *3*(1), 235–245.

[71] Kutyłowski, M., Hanzlik, L., & Kluczniak, K. (2016). Pseudonymous signature on eIDAS token—Implementation based privacy threats. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9723*, 467–477.

[72] Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In A. Chugunov, I. Khodachek, Y. Misnikov, & D. Trutnev (Eds.), *Electronic Governance and Open Society: Challenges in Eurasia* (pp. 75–89). Springer International Publishing.

[73] Logius. (2021). *DigiD. Login methods. Identity card*. https://www.digid.nl/en/login-methods/identity-card

[74] McKinsey Global Institute. (2019). *Digital identification: A key to inclusive growth*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth#

[75] Ministry of Digital Affairs. (2020). *Gov.pl. ID card—Information*. https://www.gov.pl/web/gov/dowod-osobisty-informacje

[76] Ministry of Digital Affairs. (2021a). *Gov.pl. Login. Wybierz sposób logowania*. https://login.gov.pl/login/login?ssot=wtkck6qdrhxwjz8msmze

[77] Ministry of Digital Affairs. (2021b). *Profil Zaufany. Jak chcesz uzyskać Profil Zaufany*. https://pz.gov.pl/pz/registerMainPage?ssot=zq2lfzp18ivhbz9tjnmd

[78] Ministry of Digital Governance. (2021). *Govgr. Identity documents. Mailbox*. https://www.gov.gr/ipiresies/polites-kai-kathemerinoteta/stoikheia-polite-kai-tautopoietika-eggrapha

[79] Ministry of Digitalisation. (2021a). *Guichet.lu. MyGuichet.lu. Log in*. https://guichet.public.lu/en/myguichet.html

[80] Ministry of Digitalisation. (2021b). *Guichet.public.lu. Citizens.Citizenship. Identity apers. ID card*. https://guichet.public.lu/en/citoyens/citoyennete/papiers-identite/carte-identite/nouv-carte-identite-adulte.html#bloub-10

[81] Ministry of the Interior. (2020). *Citizen Portal. Log in to the Citizen Portal*. https://obcan.portal.gov.cz/prihlaseni

[82] Ministry of the Interior. (2021). *DNI electrónico. Ideas básicas*. https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_100&id_menu=1

[83] Ministry of the Interior of the Czech Republic. (2018). *Notification form for electronic identity scheme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Czech+Republic

[84] Morgner, F., Bastian, P., & Fischlin, M. (2016a). Attribute-based access control architectures with the eIDAS protocols. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10074*, 205–226.

[85] Morgner, F., Bastian, P., & Fischlin, M. (2016b). Securing transactions with the eIDAS protocols. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9895*, 3–18.

[86] MTITC. (2021). *Ministry of Transport, Information Technology and Communications. Информационни технологии. Цифрова България*. https://www.mtitc.government.bg/bg/category/85

[87] National Agency for Network and Electronic Services. (2021). *slovensko.sk. Login through slovensko.sk*. https://prihlasenie.slovensko.sk/oamfed/idp/samlv20?lng=en&SAMLRequest=7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvvvfe6O51OJ%2fff%2fz9cZmQBbPbOStrJniGAqsgfP358Hz8iHh%2bv2%2fnyVf6L1nnTpu8W5bJ59K4pPvto3rarR3fvXl1dja%2fujav64u7ezs7u3d%2f7i%2bevp%2fN8kW0Xy6bNltP8I%2fvW7Oa3PkrPnn720e%2bfTfKde5%2fm2fb5%2bcFke%2f%2f84Wz74Pz%2bp9v5ZH9%2f%2f%2bD%2bwYN7%2bw8%2bSn8yr5uiWn720d5456P0KSFYLLOWP0E%2fDXW0qot5mTX5ssjHTVld5svmbTVu3t6tssV5PrtbzFZ3m2xRXu7t%2fB7l8uKzfEkYNM06P2PsW4K9s7e7vXNve%2b%2fhm937j%2b4%2fpP%2bNP32481M6rM8%2bWtfLR1XWFM2jZbbIm0ft9NHr4y%2bePyKkHq3qqq2mVfn

R0WOGWt%2fmpaxp8hrD%2bOjIDAP08tF%2ffFfAHT2%2b68%2fP0f8D&SigAlg=http%3a%2f%2fwww.w3.org%2f2000%2f09%2fxmldsig%23rsa-sha1&Signature=OuWVXKuaYZUpL9opO27LIasriiTcHtaF%2bvcwNuP46%2btWYzENXVI6xzO3OEic%2fPt5gvBSkKli6KvxJD1nl%2b17BPPXBuOsMLT3REB3nWLbJPF99FFFCuzG4uHUxMuXWXdRBkK8F5bQ4VJuiMfTwG%2fB7idPZ25CAu1QJBqZ4HEdfiG1kAlRLjGPD3fBMCKsa41G7v7rANDGGFd4MPjmei7FL6tDTEbhR8L1fC7f5hPD6lQvXEib1ccEz%2boOqbEgEABnTEplf%2f5f6yqex02M%2bqk%2baLZ0CmubVKWinAN%2f7ObWKuKe9OwchKxy5XtQxaeGA%2beOe5a4giklThANbg6Wzb4xDg%3d%3d

[88] Neubauer, T., & Heurix, J. (2010). A Roadmap for Personal Identity Management. *2010 Fifth International Conference on Systems*, 134–139.

[89] Nguyen, K. (2018). Certification of eIDAS trust services and new global transparency trends. *Datenschutz Und Datensicherheit - DuD*, *42*(7), 424–428.

[90] NISZ Zrt. (2021). *SZÜF Portal. Bejelentkezes.* https://magyarorszag.hu/szuf_fooldal#fooldal

[91] Novak, A. (2018). *Gov.pl. Login.gov.pl.* https://login.gov.pl/login/news#news1

[92] Pelikánová, R. M., Cvik, E. D., & MacGregor, R. (2019). Qualified electronic signature – EIDAS striking Czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, *67*(6), 1551–1560.

[93] Polanski, P. P. (2015). Towards the single digital market for e-identification and trust services. *The Computer Law and Security Report*, *31*(6), 773–781.

[94] Public broadcasting of Latvia. (2019). *New style ID cards to be issued from September in Latvia*. https://eng.lsm.lv/article/society/society/new-style-id-cards-to-be-issued-from-september-in-latvia.a330132/

[95] QSR International. (2020). *NVIVO. Fueling Academic Research.* https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/

[96] Regulation 910/2014. (2014). *On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. European Parliament, Council of the European Union. http://data.europa.eu/eli/reg/2014/910/oj

[97] Regulation 2018/1724. (2018). *Establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. OJ L 295, 21.11.2018, p. 1–38*. http://data.europa.eu/eli/reg/2018/1724/oj

[98] Revenue Irish Tax an Customes department. (2021). *MyAccount. What do I need to register?* https://www.ros.ie/myaccount-web/register.html?execution=e1s1

[99] Ribeiro, C., Leitold, H., Esposito, S., & Mitzam, D. (2018). STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security*, *17*(5), 569–585.

[100] Roelofs, (sup) Verheul, & Jacobs. (2019). *Analysis and comparison of identification and authentication systems under the eIDAS regulation. Institute for Computing and Information Sciences, Radboud University.*

[101] Servizz.gov Agency. (2021). *Servizz.gov.mt.Your online guide to government services. ID login*. https://www.servizz.gov.mt/en/Pages/default.aspx

[102] Smeets. (2018). *Notification form Belgian eID Scheme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Belgium+-+eID

[103] Smeets. (2019). *Notification form Belgian FAS itsme*. https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Belgium+-+Itsme

[104] Smiraglia, P., De Benedictis, M., Atzeni, A., Lioy, A., & Pucciarelli, M. (2017). The FICEP infrastructure: How we deployed the italian eidas node in the cloud. *Communications in Computer and Information Science*, *792*, 196–210.

[105] State Regional Development Agency. (2021). *Latvian State Portal. E-services*. https://latvija.lv/Epakalpojumi

[106] Stevens, T., Hoikkanen, A., & Elliott, J. (2010). *The state of the electronic identity market. Technologies, infrastructure, services and policies*. Institute for Prospective Technological Studies (Joint Research Centre). DOI: 10.2791/4851

[107] Swedish Companies Registration Office. (2021). *Verksamt.se. Select login option*. https://www.verksamt.se/web/international/login?entityID=https%3A%2F%2Fwww.verksamt.se%2Fshibboleth%2Fmetadata&return=https%3A%2F%2Fwww.verksamt.se%2FShibboleth.sso%2Flogin%3FSAMLDS%3D1%26target%3Dss%253Amem%253A441b0fb1ea0624db728d9558e1936b84485bb66adfc0e2cb98ede2c89d7b3991

[108] Trust Service Authority of Slovenia. (2020). *SI-TRUST. Authentication and e-Signature Service SI-PASS*. https://www.si-trust.gov.si/en/si-pass/

[109] Tsap, V., Lips, S., & Draheim, D. (2020a). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In A. Kő, E. Francesconi, G. Kotsis, A. M. Tjoa, & I. Khalil (Eds.), *Electronic Government and the Information Systems Perspective* (pp. 159–173). Springer International Publishing.

[110] Tsap, V., Lips, S., & Draheim, D. (2020b). eID Public Acceptance in Estonia: Towards Understanding the Citizen. *21st Annual International Conference on Digital Government Research*, 340–341.

[111] Tsap, V., Pappel, I., & Draheim, D. (2019). Factors Affecting e-ID Public Acceptance: A Literature Review. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11709*, 176–188.

[112] Turkanovic, M., & Podgorelec, B. (2020). Signing Blockchain Transactions Using Qualified Certificates. *IEEE Internet Computing*, *24*(6), 37–43.

[113] Valtna-Dvořák. (2020). *Master's Degree (2020). (Sup) Dirk Draheim; Valentyna Tsap, ROCA Vulnerability and State Provided Electronic Identification: Case of Estonia, Tallinn University of Technology School of Information Technologies, Department of Software Science*.

[114] van Dijck, J., & Jacobs, B. (2020). Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, *22*(5), 896–914.

[115] VAS "Latvijas Valsts radio un televīzijas centrs". (2017). *eParaksts. About eSignature*. https://www.eparaksts.lv/en/About_eSignature

[116] Veerpalu, A., Jürgen, L., Rodrigues e Silva, E. da C., & Norta, A. (2020). The hybrid smart contract agreement challenge to European electronic

signature regulation. *International Journal of Law and Information Technology*, *28*(1), 39–84.

[117] Yin. (2018). *Case study research and applications: Design and methods* (Sixth edition.). SAGE.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Natalia Vinogradova

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Re-shaping the eIDAS Regulation from Stakeholder´s Perspective, supervised by Silvia Lips
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 - List of EU Member States that pre-notified and notified eID schemes

No	EU member countries	Pre-notified eID schemes (eID User Community, 2019a)	Notified eID schemes (eID User Community, 2019a)
1	Austria	-	-
2	Belgium	-	Belgian eID Scheme FAS / eCards; Belgian eID Scheme FAS / Itsme® (mobile App)
3	Bulgaria		-
4	Croatia	-	National Identification and Authentication System (NIAS)
5	Cyprus		-
6	Czechia	-	National identification scheme of the Czech Republic
7	Denmark	-	NemID
8	Estonia	-	Estonian eID scheme: ID card; Estonian eID scheme: RP card; Estonian eID scheme: Digi-ID; Estonian eID scheme: e-Residency Digi-ID; Estonian eID scheme: Mobiil-ID; Estonian eID scheme: diplomatic identity card
9	Finland	-	-

No	EU member countries	Pre-notified eID schemes (eID User Community, 2019a)	Notified eID schemes (eID User Community, 2019a)
10	France	FranceConnect+ / The Digital Identity La Poste	-
11	Germany	-	German eID based on Extended Access Control
12	Greece	-	-
13	Hungary	-	Estonian eID scheme: diplomatic identity card
14	Ireland	-	-
15	Italy	-	Italian eID based on National ID card (CIE); SPID – Public System of Digital Identity
16	Latvia	-	Latvian eID scheme (eID)
17	Lithuania	-	Lithuanian National Identity card (eID / ATK)
18	Luxembourg	-	Luxembourg national identity card (eID card)
19	Malta	Identity Malta	-
20	Netherlands	-	DigiD; Trust Framework for Electronic Identification (Afsprakenstelsel Elektronische Toegangsdiensten)
21	Poland	-	-

No	EU member countries	Pre-notified eID schemes (eID User Community, 2019a)	Notified eID schemes (eID User Community, 2019a)
22	Portugal	Sistema de Certificação de Atributos Profissionais - Professional Attributes Certification System	Chave Móvel Digital - Digital Mobile Key; Cartão de Cidadão - Portuguese national identity card
23	Romania	-	-
24	Slovakia	-	National identity scheme of the Slovak Republic
25	Slovenia	-	-
26	Spain	-	Documento Nacional de Identidad electrónico (DNIe) - Spanish ID card (DNIe)
27	Sweden	Swedish eID (Svensk elegitimation)	-

Appendix 3 - Cases. Stakeholders: Public sector

Stakeholders: Public sector	**Country of origin**	**Organisation size**	**Scope**
Cases\\F547048 Public authority CNNum France	EU	Small	National
Cases\\F547510 Ministry of Social Affairs and Health Finland	EU	Large	National
Cases\\F547522 Public authority Organisation City of Amsterdam	EU	Large	Local
Cases\\F548621 Tallinn University of Technology Estonia	EU	Large	Academic, research Institution
Cases\\F548999 Poste Italiane	EU	Large	Not Applicable
Cases\\F549050 Academic research Institution. Spain	EU	Large	Academic, research Institution
Cases\\F549054 CNIL French Data Protection Authority	EU	Medium	National

Appendix 4 - Cases. Stakeholders: Private sector

Stakeholders Private sector	Country of origin	Organisation size	User type
Cases\\F540380 idnow Germany	EU	Medium	Company, business organisation
Cases\\F543642 Yubico AB Sweden	EU	Large	Company, business organisation
Cases\\F544741 CLR Labs France	EU	Micro	Company, business organisation
Cases\\F545872 Association for promotion of digital verification Norway	Non-EU	Micro	Business association
Cases\\F546495 Bundesdruckerei GmbH Germany	EU	Large	Company, business organisation
Cases\\F546747 OneSpan, Inc.United States	Non-EU	Large	Company, business organisation
Cases\\F547018 Business association Finance Denmark	EU	Medium	Business association
Cases\\F547025 Business association eco - Verband der Internetwirtschaft e.V. Germany	EU	Small	Business association

Stakeholders Private sector	**Country of origin**	**Organisation size**	**User type**
Cases\\F547352 BvDP Germany	EU	Micro	Company, business organisation
Cases\\F547377 Developers Alliance United States	Non-EU	Micro	Business association
Cases\\F547499 ORANGE France	EU	Large	Company, business organisation
Cases\\F547552 European Signature Dialog Austria	EU	Small	Company, business organisation
Cases\\F548611 1&1 Germany	EU	Large	Company, business organisation
Cases\\F548633 Onfido Ltd UK	Non-EU	Large	Company, business organisation
Cases\\F548665 Deutsche Telekom AG Belgium	EU	Large	Company, business organisation
Cases\\F548675 Alliance for Digital Trust France	EU	Micro	Business association
Cases\\F548762 FIDO Alliance United States	Non-EU	Micro	Company, business organisation

Stakeholders Private sector	**Country of origin**	**Organisation size**	**User type**
Cases\\F548763 Better Identity Coalition United States	Non-EU	Micro	Company, business organisation
Cases\\F548844 CONSULTING – EVROTRUST France	EU	Small	Company, business organisation
Cases\\F548866 Civil-law Notaries Netherlands	EU	Medium	Business association
Cases\\F548902 private sector stakeholder	Not Applicable	Not Applicable	Company, business organisation
Cases\\F548913 ITFA Switzerland	Non-EU	Micro	Business association
Cases\\F548927 Business association Insurance Europe Belgium	EU	Small	Business association
Cases\\F548968 Erste Group Bank AG Austria	EU	Large	Company, business organisation
Cases\\F548993 Thales DIS France	EU	Large	Company, business organisation
Cases\\F548996 Legal Studio Belgium	EU	Small	Company, business organisation

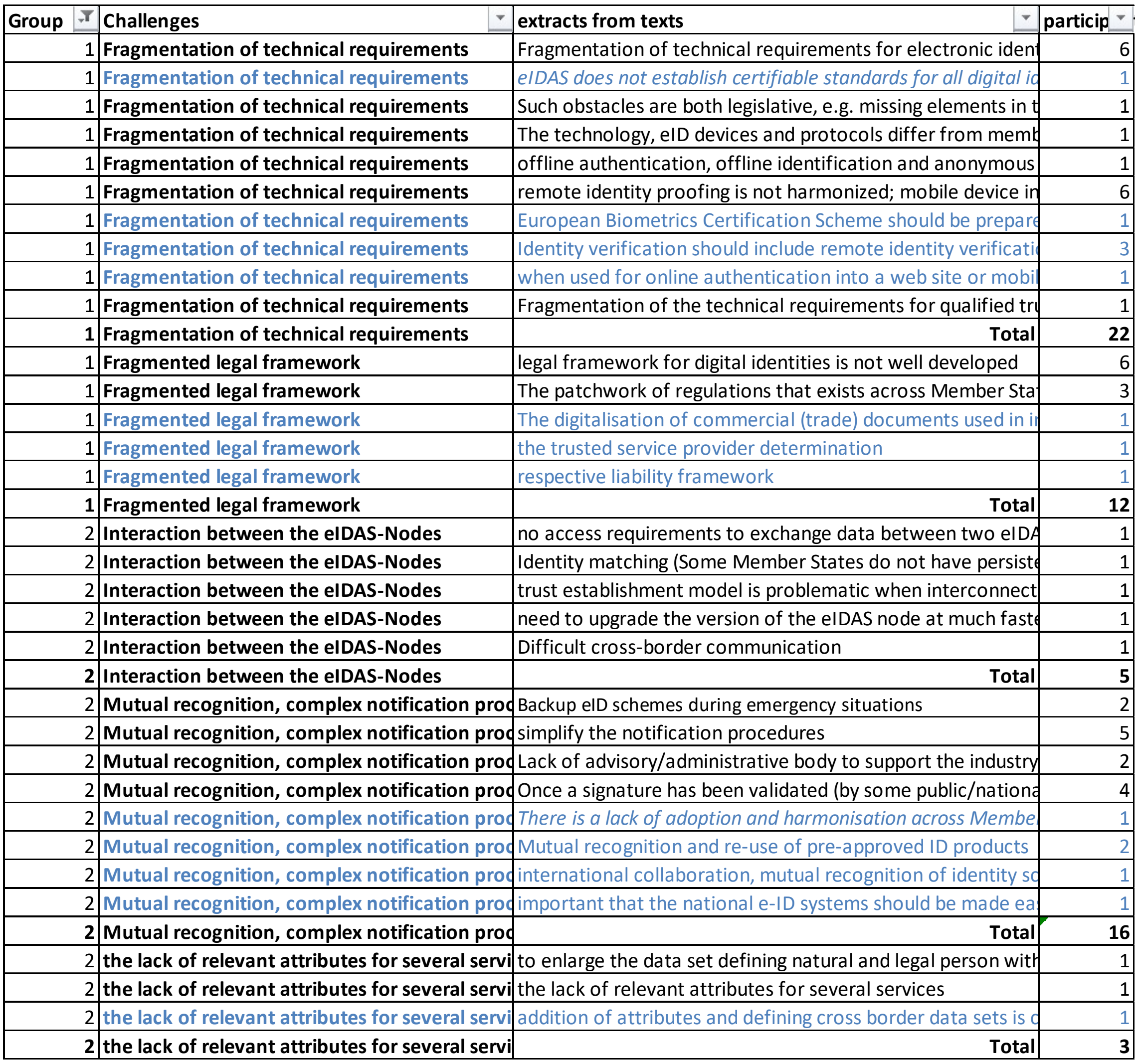
Stakeholders Private sector	**Country of origin**	**Organisation size**	**User type**
Cases\\F549006 Eurosmart Belgium	EU	Micro	Business association
Cases\\F549007 Business association Switzerland	Non-EU	Micro	Business association
Cases\\F549030 EPIF	EU	Micro	Company, business organisation
Cases\\F549055	EU	Not Applicable	Company, business organisation
Cases\\F549060 ARIADNEXT	EU	Medium	Company, business organisation

Appendix 5 - Cases. Stakeholders: Others

Stakeholders Others	Country of origin	User type
Cases\\F539174	Unassigned	Anonymous
Cases\\F539560 EU citizen Czech Republic	EU	EU citizen
Cases\\F541541	Unassigned	Anonymous
Cases\\F543486	Unassigned	Anonymous
Cases\\F543707 EU citizen Italy	EU	EU citizen
Cases\\F543935 EU citizen France	EU	EU citizen
Cases\\F547234 NGO Center for Data Innovation United States	Non-EU	NGO
Cases\\F547545 NGO GLEIF Switzerland	Non-EU	NGO
Cases\\F547568 NGO Visible Digital Seal International Council France	EU	NGO
Cases\\F548663 Superior Council of Notaries France	EU	Not Applicable
Cases\\F548781 EU citizen Italy	EU	EU citizen
Cases\\F548915 GISAD i.G. Germany	EU	Not Applicable
Cases\\F548950 Italy	EU	Anonymous
Cases\\F548957 EU citizen France	EU	EU citizen
Cases\\F548976 NGO OpenID Foundation Germany	EU	NGO

Appendix 6 – Coding: private sector (1)

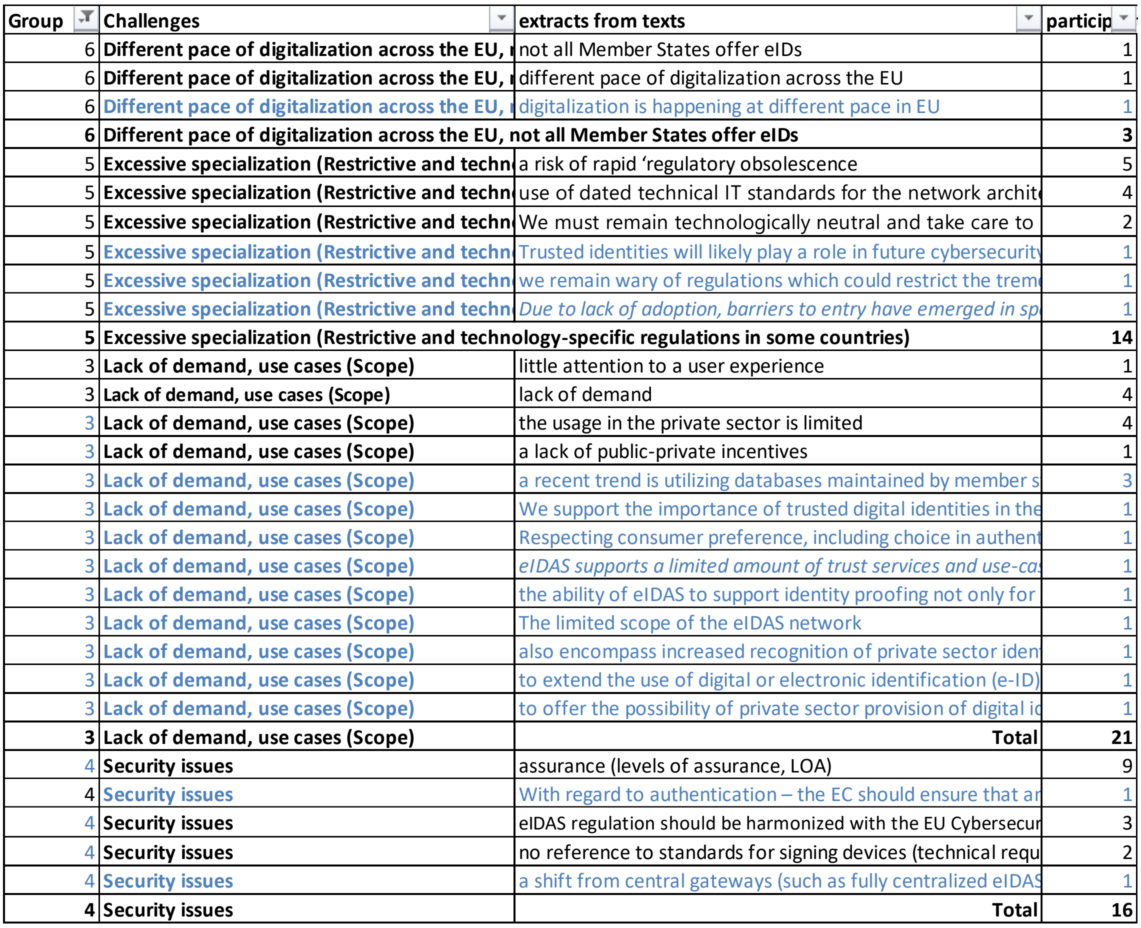
Source: Published initiatives. EU digital ID scheme for online transactions across Europe (EC, 2020b)



Group	Challenges	extracts from texts	particip
1	**Fragmentation of technical requirements**	Fragmentation of technical requirements for electronic ident	6
1	**Fragmentation of technical requirements**	*eIDAS does not establish certifiable standards for all digital id*	1
1	**Fragmentation of technical requirements**	Such obstacles are both legislative, e.g. missing elements in t	1
1	**Fragmentation of technical requirements**	The technology, eID devices and protocols differ from memb	1
1	**Fragmentation of technical requirements**	offline authentication, offline identification and anonymous	1
1	**Fragmentation of technical requirements**	remote identity proofing is not harmonized; mobile device in	6
1	**Fragmentation of technical requirements**	European Biometrics Certification Scheme should be prepare	1
1	**Fragmentation of technical requirements**	Identity verification should include remote identity verificati	3
1	**Fragmentation of technical requirements**	when used for online authentication into a web site or mobil	1
1	**Fragmentation of technical requirements**	Fragmentation of the technical requirements for qualified tru	1
1	**Fragmentation of technical requirements**	**Total**	**22**
1	**Fragmented legal framework**	legal framework for digital identities is not well developed	6
1	**Fragmented legal framework**	The patchwork of regulations that exists across Member Sta	3
1	**Fragmented legal framework**	The digitalisation of commercial (trade) documents used in i	1
1	**Fragmented legal framework**	the trusted service provider determination	1
1	**Fragmented legal framework**	respective liability framework	1
1	**Fragmented legal framework**	**Total**	**12**
2	**Interaction between the eIDAS-Nodes**	no access requirements to exchange data between two eIDA	1
2	**Interaction between the eIDAS-Nodes**	Identity matching (Some Member States do not have persiste	1
2	**Interaction between the eIDAS-Nodes**	trust establishment model is problematic when interconnect	1
2	**Interaction between the eIDAS-Nodes**	need to upgrade the version of the eIDAS node at much faste	1
2	**Interaction between the eIDAS-Nodes**	Difficult cross-border communication	1
2	**Interaction between the eIDAS-Nodes**	**Total**	**5**
2	**Mutual recognition, complex notification proc**	Backup eID schemes during emergency situations	2
2	**Mutual recognition, complex notification proc**	simplify the notification procedures	5
2	**Mutual recognition, complex notification proc**	Lack of advisory/administrative body to support the industry	2
2	**Mutual recognition, complex notification proc**	Once a signature has been validated (by some public/nationa	4
2	**Mutual recognition, complex notification proc**	*There is a lack of adoption and harmonisation across Membe*	1
2	**Mutual recognition, complex notification proc**	Mutual recognition and re-use of pre-approved ID products	2
2	**Mutual recognition, complex notification proc**	international collaboration, mutual recognition of identity sc	1
2	**Mutual recognition, complex notification proc**	important that the national e-ID systems should be made ea	1
2	**Mutual recognition, complex notification proc**	**Total**	**16**
2	**the lack of relevant attributes for several servi**	to enlarge the data set defining natural and legal person with	1
2	**the lack of relevant attributes for several servi**	the lack of relevant attributes for several services	1
2	**the lack of relevant attributes for several servi**	addition of attributes and defining cross border data sets is c	1
2	**the lack of relevant attributes for several servi**	**Total**	**3**

Appendix 6 – Coding: private sector (2)

Source: Published initiatives. EU digital ID scheme for online transactions across Europe (EC, 2020b)



Group	Challenges	extracts from texts	particip
6	**Different pace of digitalization across the EU, n**	not all Member States offer eIDs	1
6	**Different pace of digitalization across the EU, n**	different pace of digitalization across the EU	1
6	**Different pace of digitalization across the EU, n**	digitalization is happening at different pace in EU	1
6	**Different pace of digitalization across the EU, not all Member States offer eIDs**		**3**
5	**Excessive specialization (Restrictive and techn**	a risk of rapid ‘regulatory obsolescence	5
5	**Excessive specialization (Restrictive and techn**	use of dated technical IT standards for the network archit	4
5	**Excessive specialization (Restrictive and techn**	We must remain technologically neutral and take care to	2
5	**Excessive specialization (Restrictive and techn**	Trusted identities will likely play a role in future cybersecurity	1
5	**Excessive specialization (Restrictive and techn**	we remain wary of regulations which could restrict the trem	1
5	**Excessive specialization (Restrictive and techn**	*Due to lack of adoption, barriers to entry have emerged in sp*	1
5	**Excessive specialization (Restrictive and technology-specific regulations in some countries)**		**14**
3	**Lack of demand, use cases (Scope)**	little attention to a user experience	1
3	**Lack of demand, use cases (Scope)**	lack of demand	4
3	**Lack of demand, use cases (Scope)**	the usage in the private sector is limited	4
3	**Lack of demand, use cases (Scope)**	a lack of public-private incentives	1
3	**Lack of demand, use cases (Scope)**	a recent trend is utilizing databases maintained by member s	3
3	**Lack of demand, use cases (Scope)**	We support the importance of trusted digital identities in the	1
3	**Lack of demand, use cases (Scope)**	Respecting consumer preference, including choice in authent	1
3	**Lack of demand, use cases (Scope)**	*eIDAS supports a limited amount of trust services and use-ca*	1
3	**Lack of demand, use cases (Scope)**	the ability of eIDAS to support identity proofing not only for	1
3	**Lack of demand, use cases (Scope)**	The limited scope of the eIDAS network	1
3	**Lack of demand, use cases (Scope)**	also encompass increased recognition of private sector iden	1
3	**Lack of demand, use cases (Scope)**	to extend the use of digital or electronic identification (e-ID)	1
3	**Lack of demand, use cases (Scope)**	to offer the possibility of private sector provision of digital i	1
3	**Lack of demand, use cases (Scope)**	**Total**	**21**
4	**Security issues**	assurance (levels of assurance, LOA)	9
4	**Security issues**	With regard to authentication – the EC should ensure that ar	1
4	**Security issues**	eIDAS regulation should be harmonized with the EU Cybersecur	3
4	**Security issues**	no reference to standards for signing devices (technical requ	2
4	**Security issues**	a shift from central gateways (such as fully centralized eIDAS	1
4	**Security issues**	**Total**	**16**

Appendix 7 – Coding: public sector

	First group		Second group			Third group	Forth group	Fifth group	Sixth group
Stakeholders: Public sector	**Fragmented legal framework**	**Fragmented tech. requirements**	**Mutual recognition**	**Interaction between the eIDAS-Nodes**	**Lack of relevant attributes**	**Limited scope of the eIDAS**	**Security and privacy issues**	**Excessive specialization**	**Different pace of digitization**
Cases\\F547048 Public authority CNNum France	1	1	1			1	1		
Cases\\F547510 Ministry of Social Affairs and Health Finland									
Cases\\F547522 Public authority Organisation City of Amsterdam							1		
Cases\\F548621 Tallinn University of Technology Estonia		1							
Cases\\F548999 Poste Italiane	1					1	1		
Cases\\F549050 Academic research Institution. Spain	1	1				1		1	
Cases\\F549054 CNIL French Data Protection Authority	1						1		
Total	**4**	**3**	**1**	**0**	**0**	**3**	**4**	**1**	**0**

Appendix 8 – Coding: others

	First group		Second group			Third group	Forth group	Fifth group	Sixth group
Stakeholders Others	**Fragmented legal framework**	**Fragmented tech. requirements**	**Mutual recognition**	**Interaction between the eIDAS-Nodes**	**Lack of relevant attributes**	**Limited scope of the eIDAS**	**Security and privacy issues**	**Excessive specialization**	**Different pace of digitization**
Cases\\F539174		1				1			
Cases\\F539560 EU citizen Czech Republic		1				1			
Cases\\F541541						1			
Cases\\F543486	1		1						
Cases\\F543707 EU citizen Italy			1					1	
Cases\\F543935 EU citizen France					1		1		
Cases\\F547234 NGO Center for Data Innovation United States	1	1				1			
Cases\\F547545 NGO GLEIF Switzerland	1			1	1	1	1		
Cases\\F547568 NGO Visible Digital Seal International Council France		1	1						
Cases\\F548663 Superior Council of Notaries France		1			1				
Cases\\F548781 EU citizen Italy	1	1			1				1
Cases\\F548915 GISAD i.G. Germany							1		
Cases\\F548950 Italy		1				1	1		
Cases\\F548957 EU citizen France					1		1		
Cases\\F548976 NGO OpenID Foundation Germany		1			1	1			
	4	**8**	**3**	**1**	**6**	**7**	**5**	**1**	**1**

Appendix 9 – The short list of proposed recommendation

Source: Published initiatives. EU digital ID scheme for online transactions across Europe (EC, 2020b)

Category	Challenges	Solutions
Fragmented technical requirements	lack of common technical standards for digital identity matters	to involve European Standard Organizations to complete the current set of standards
	process to certify a signature creation device is cumbersome and brings to an odd and fragmented situation	ENISA should define a unique scheme for security certification of devices, shaped around the already existing and accepted international security schemes
	offline authentication, offline identification and anonymous authentication, other mobile device interactions and remote onboarding are not harmonized	Harmonize evaluation of alternative methods and certification processes, especially for new authentication solutions
		specify the minimum criteria relating to remote identification
		determine the identification of devices and the Internet of Things procedures
Fragmented legal framework	national rules of the Member States stay fragmented and undeveloped	framework needs to be more prescriptive on the EU level
		Produce and publish implementing acts to create interoperability with transitional arrangements and transition time for existing certificates and systems on the market
Limited scope of the eIDAS network and use cases	lack of demand	draw attention to a user experience, respect consumer preference, including choice in authentication; promote the use of trusted identities for all Europeans
	lack of use cases	allow eIDAS to be used by the private sector
		encompass increased recognition of private sector identity providers
	identities of legal persons, professionals	EUid could be created for the identities of legal persons
		Mandatory use of Legal Entity Identifier (LEI)
		Create an eIDAS identity for companies and professionals

Category	**Challenges**	**Solutions**
Security and privacy issues	too much space for interpretation in the levels of assurance	eIDAS regulation should be harmonized with the EU Cybersecurity Act
		Incorporate principles: privacy by design, decentralized architecture, data minimization; organize courses for citizens
		Create rules for private trust service providers
Mutual recognition	complex notification procedures	standardize the peer-review procedure
		If a product has been approved for use with an eID scheme in one EU member state, the same product should be allowed to be re-approved for other eID schemes.
	lack of advisory/administrative body to support the industry by implementing eIDAS	An institution should be created in which supervisory bodies can coordinate their activities in order to ensure a common interpretation of the eIDAS regulation
	supervisory bodies have no legal enforcing authority	Create a set of baselines of auditing rules and a baselines audit plan
		Standardize accreditation process for Conformity assessment Bodies
	not clear management of emergencies	include "Backup eID schemes" for emergencies
		international collaboration, mutual recognition of identity schemes with non-EU financial centres, third countries
Excessive specialization	insufficient consideration of innovative solutions	existing Single Sign-On standards should be included
		Any proposed revisions must take into account the dynamic and evolving nature of the digital economy and the infrastructure it rides on.
	regulations are "restrictive and technology-specific"	the qualification should be more abstract, so that emerging electronic identity and trust services technologies could qualify