Stefan Dedovic

Cross-border eID enactment in the EU
The case of Belgium and Estonia

Master Thesis

at the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

Supervisor:	Prof. dr. ir. Joep Crompvoets
Co-supervisor:	Prof. dr. dr. Robert Krimmer
Presented by:	Stefan Dedovic stefan.dedovic@hotmail.com

Date of Submission: 2021-08-09

Acknowledgements

September 9th 2019, was when I first arrived in Leuven, Belgium, to begin my journey towards a Masters degree. I would like to say that I could not imagine a better personal development that I had during the two years time. During this, for me, extraordinary trip, I was surrounded by amazing young and bright-minded people who were on the same mission as me. Therefore, I would like to express how grateful I am to be a part of an amazing group of students and professors in the PIONEER programme. Being able to meet young and bright-minded people from around the world is, for me, a fantastic success that fills me with gratitude and beautiful emotions.

Firstly, I would like to thank my family who have always supported me throughout this incredible journey. They have been continuously helping me and supporting me emotionally through tough times far away from home. Also, to my closest friends back home, who spent many hours on WhatsApp calls with me. They helped me to feel less nostalgic and to realize once again how lucky I am to have them.

I owe a deep sense of gratitude and admiration to my supervisors Prof. Joep Crompvoets and Prof. Robert Krimmer. Their extraordinary support and kind assistance inspired me throughout the whole process of writing this thesis. I am fortunate to be able to learn and have many conversations with amazing persons and exceptional scholars. Also, I would like to mention how grateful I am to interviewee experts who took the time to have a conversation with me and provide their valuable knowledge and insights about this exciting topic. Without their involvement, this research would not have achieved set objectives.

Finally, I would like to say that this acknowledgement is not the last one. I am sure there will be a time in future that our paths cross again. I look forward to new incredible journeys and future successes that are ahead of me.

Abstract

There is a lack of mutual recognition of nationally issued eID means across the EU. As a result, the inability to electronically identify using national issued electronic identity cards affects at least 150 million people living in the EU. Thus, the EU and the Member States are working on enabling electronic identification across borders. eIDAS regulation, adopted in 2014, was the first step to achieve mutual recognition of eIDs in the EU. However, seven years later, set objectives of eIDAS regulation were not achieved. Thus, this research aims to explore and gain insights of existing factors that affect cross-border eID enactment from a national perspective.

Furthermore, this research aims to analyse existing perspectives on the new eIDAS proposal and European Digital Identity Wallet. The set objectives of this research are to analyse existing factors and find commonalities and differences among digitally advanced countries in the EU. Hence, utilizing a qualitative research method with multiple case study analyses, this research focuses on Estonia and Belgium as digitally advanced case-study countries. Through primary and secondary data analysis, identified factors are classified under technological, organisational and institutional dimensions. Finally, research findings show that the institutional approach towards unique and personal identifiers and cross-border data sharing in the EU has a significant impact on cross-border eID enactment.

Content

List of Figures

List of Tables

1 Introduction

Identification is present among people throughout history. In the historical times, during which the social communities and social interactions were on a small scale, identification among people was based on personal recognition and trust (M. Lips, 2008). Moreover, it was based on the vocal recognition in some communities as well. For example, in Maori culture, members of the group have been identifying themselves by reciting “Whakapapa” (Whakapapa Maori, n.d). Whakapapa is a way of identifying a person in Maori culture, and its meaning is “to place in layers, one upon another” (Whakapapa Maori, n.d). A person reciting Whakapapa proclaims its Maori identity and, by that, links to the ancestors and the tribal community (Whakapapa Maori, n.d).

After the social and economic development, people were extending their communities and, hence, developing the more complex political organisation, which consequently required changes in identification. With the development and expansion of the bureaucratic society, the identification changed into the process where people need to present paper-based proof of identity in order to identify themselves (M. Lips, 2008). Generally, in the 20th century, the expansion of government citizens' identifications practices have emerged. This expansion can be explained, *inter alia,* among two crucial developments.

First is the creation and development of the social citizenship rights and entitlements, which was provided by separate public services (M. Lips, 2008). Hence, this resulted in the siloed administrations in the countries, keeping specific data in sector-specific databases. The identification of the citizens is necessary to provide the right services and social benefits to the right people. The second reason for the expansion of the identification practices in the countries is the expansion of globalisation (M. Lips, 2008). Globalisation emerged with an increasingly mobile society, which resulted in creating the travel identification document, passport (M. Lips, 2008). According to M. Lips (2008), the issuance of passports gave the states exclusive power and the right to authorise and regulate the movement of people. This development of the identification practices led governments to strict rules and practices in the identification management systems of their citizens.

The changes in the public administrations' practices at the end of the 20th century and the rapid development of information and communication technologies (ICT) led to significant reforms in identity management. The utilization of ICTs was also started to be implemented in the identification management systems within the countries. With reforms in the service provision towards the more digital provision of services, citizens were required to identify online, hence enabling benefits from specific services.

Consequently, the countries started developing electronic identification management systems (eIDMS) (M. Lips, 2008). However, the design and implementation of the eIDMS were different among countries, isolated on country-specific needs and problems. Hence, the isolated design and implementation of the electronic identity (eID)[1] caused highly heterogenic eIDMS. The heterogeneity of the eIDMS among countries is particularly important in the European Union (EU) due to the integration motives of the EU members.

More specifically, with the creation of the European Economic Community (EEC) in 1957 and the Treaty of Rome, it is envisioned to "erase" internal borders across the community and enable free movement of citizens, goods and capital. Therefore, high-level cooperation and proper governance among MS are required to achieve the envisioned objective.

1.1 Research motivation and relevance

Cross-border cooperation, EU integration and provision of public services across borders in the EU is an integral element of the EU single market success. As one of the EU's greatest achievements, the European single market stimulates economic growth, reduces inequalities, and enables the free movement of goods, services, and people (European Commission, 2021a). In order to more develop the EU single market, Member States (MS) are incentivised to cooperate, share information and develop joint initiatives through various EU policy actions (Sousa, 2013). Consequently, this cooperation and collaboration between public administrations in the EU resulted in the growth of demand for cross-border services (Peristeras, Tarabanis, & Loutas, 2007). Thus, the development of cross-border services can lead to various benefits to businesses and citizens. These benefits are enhanced competitiveness, reduced administrative burden, savings in costs and time, and last but not least, enhanced cultural, political and social integration in the EU (ESPON, 2020; Peristeras et al., 2007). The main goal of this "Europeanisation" is to allow citizens, businesses, and public administrations to interact and exercise rights seamlessly without any barriers.

Provision of the cross-border services has also contributed to the economic and employment growth in the EU (Fritsch & Bertenrath, 2019). In total, around 10 million jobs, which is around 5% of the total employment in the EU, are dependent on cross border services (Fritsch & Bertenrath, 2019). Compared to the beginning of the 2000s, this is a significant increase which shows the importance of cross-border service

[1] In this research concepts such as electronic identity and digital identity are used interchangeably.

provisioning for the labour market in the EU (Fritsch & Bertenrath, 2019). In addition, there is an increase in the employment of cross-border workers in the last few years, according to the “Annual Report on Intra-EU Labour Mobility in 2020” (Fries-Tersch, Jones, & Siöland, 2021). Fries-Tersch et al. (2021) emphasise that in 2020 there were 1.9 million cross-border workers and 3 million citizens cross-border posted workers in the EU. Moreover, around 30% of the EU population, around 150 million citizens, lives in the EU's internal border regions (Halmos, 2018). Therefore, for these citizens and others who want to study, work, retire, or start a business in another country, provision of easy access to procedures and services across the EU is essential.

Citizens are usually required to be physically present to interact with foreign public administration and to access cross-border procedures (Badinger & Maydel, 2009). The necessary physical presence might be the reason for less provision of cross-border services than the cross-border trading of goods (Badinger & Maydel, 2009). However, the rapid development of the information and communication technologies (ICT) and their deployment in the public sector promised to reduce administrative burden and improve quality, effectiveness and efficiency in public sector service provisioning (Gallo, Michele, Millard, Kåre, & Thaarup, 2014; Kalvet, Toots, & Krimmer, 2018; Veiga, Janowski, & Barbosa, 2016; Vries, Bekkers, & Tumers, 2016). Administrative burdens are considered unnecessary costs of time and money for businesses and citizens, created while interacting with the public administration (Veiga et al., 2016). Thus, reducing the administrative burden can increase savings in money and time (Cave, Botterman, Cavallini, & Volpe, 2017). One of the ways to reduce the administrative burden is to electronically exchange data between public administrations provided by the citizens only once. The once-only principle is proposition towards electronic exchanges of data provided by the citizens and business only once, between public administrations in the national and the cross-border context in the EU. It is estimated that deploying a once-only principle can lead to up to 5 billion EUR of savings, at least (Cave et al., 2017).

In 2020, the COVID-19 pandemic influenced governments for strict measures in order to reduce the impact of the health crisis. At the beginning of the pandemic, many governments worldwide, including in the EU, decided for strict measures such as lockdowns and curfews (Crahay, Di Giacomo, Chloé, Ghita, & Talpo, 2021). These decisions impacted the public administrations in the EU by causing disruptions in service provision (Crahay et al., 2021). The COVID-19 pandemic has also influenced the mobility of citizens and businesses across borders in the EU. The EU Member States decided for strict measures of closing the borders to put under control the spread of the COVID-19 virus. This decision also had a negative impact on the numerous cross-border EU citizens who were unable to exercise their regular activities across borders. As is still necessary while interacting with public administration, to be physically present and provide certified paper documents, many EU citizens could not access the cross-border public services. During the COVID-19 pandemic, it is acknowledged that the needs on the cross-border service provisions are yet not satisfied (Alonso, 2021). With the electronic data and documents exchange between public administrations across borders, the physical presence and paper documents would not be necessary anymore. Hence, achieving the electronic exchange of data and eID recognition across borders could be an important milestone for achieving full integration into the European Single Market.

During this pandemic, it is found that the level of the digital maturity of government correlates with the level of disruption in the public services provision (Crahay et al., 2021, p. 8). Leaders in the digital government transformation, such as Estonia and Denmark, experienced a very low disruption on public service provision (Cave et al., 2017). It is important to note that these countries have provided eID to their citizens and businesses. Hence, one of the important acknowledgements that the COVID-19 pandemic emphasised is the necessity and importance of eID. For example, before the pandemic in March 2020, Italy distributed around 6 million eIDs, while in March 2021, 19 million. Also, the countries that reported no disruption on the provision of public services in 2020, such as Estonia, Denmark and the Netherlands (Crahay et al., 2021), have already highly developed and widespread use of eID. Conversely, other countries were rapidly involved in the further creation of interoperability of the public services connecting with the eIDs (Crahay et al., 2021).

Establishing cross-border recognition of the eIDs in the EU has been deemed a crucial enabler for achieving the proposed benefits of the single market and digital single market (de Andrade, Monteleone, & Martin, 2013). Furthermore, the market size of the cross-border recognition of the eID in the EU is more than 2 billion euros (GSMA, 2018). In addition, there is a potential of more than 447 million users (GSMA, 2018), which can be resulted in increased entrepreneurial activity in Europe (de Andrade et al., 2013). However, the potential of the interoperable eID in the EU can only be manifested if further cooperation and sharing of best practices across the EU.

Nonetheless, eID use in cross-border situations is minimal and still in the infancy stage. The EU's eGovernment benchmark report shows that access to cross-border services is deficient (European Commission, 2020d). In the EU, less than 60% of services are offered for the citizens who want to obtain a service from another EU country, conversely to 84% of services offered for the domestic users (European Commission, 2020d). The key enabler, *inter alia*, to access the cross-border services is the eID recognition among MS.

Data on cross-border mobility emphasises that only 9% of services are accessible for cross-border users of the national eID (European Commission, 2020d).

1.2 Problem statement

The access to public services and procedures is dependent on physical presence and paper documents, as already mentioned. For cross-border workers and commuters in the EU, this presents a considerable barrier and extra burden on time and costs. For example, Estonian citizens who live in the Estonian part of the “twin city” Valga and Valka[2] and cross the border every day when commuting to work face many challenges and barriers in everyday life. As a worker under the legal jurisdiction of Latvia, an Estonian citizen, i*nter alia,* is required to fill the tax declaration and is also entitled to the pension plan of Latvia. Although living in the Estonian part of the city and being a holder of an Estonian identity card, Estonian citizens cannot identify or authenticate on the Latvian platform to access the procedures. Since it is required for citizens to securely identify and authenticate themselves to access the procedure, Estonian citizens cannot benefit from the service or access the procedures. The COVID-19 pandemic emphasised the inability and importance of the cross-border eID for many citizens of the EU.

With the goals of creating a Digital Single Market, it is required that public services are also offered for citizens of other EU MS. This requirement has caused several implications on the online service provision and the eIDMS. Many MS have adopted individual approaches for designing online public services and eID management systems. Thus, resulting in the heterogenic technological, organisational and legal ecosystem for identifying and authenticating citizens and businesses. This heterogeneity of the eIDMS and approaches led to a lack of interoperability of the eID causing the barriers for citizens and businesses to access the procedures across borders. The heterogeneity of approaches can be seen in different organisational and governance models. For example, Estonia has a centralized data exchange platform and unique and persistent personal identifiers (UPI) for each citizen and business, while in Germany, there are different data exchange platforms and no consistent UPI approach (Shehu, Pinto, & Correia, 2019). This diversity of approaches towards the development of the digital government and eID management systems causes the inability of cross-border EU citizens and businesses to access the public service with their national eID card.

To be able to access public services, nationals from other countries are required to apply for a resident ID or to obtain another eID card (i.e. BankID) (Hinsberg, Kala, Kask, &

[2] For more information, please see: https://visitvalgavalka.com/1-city-2-states/

Kutt Anders, 2020). Thus, the motivation to use national state-issued eID for cross-border services in accordance with eIDAS regulation remains low, according to Hinsberg et al. (2020). This situation requires a citizen to obtain many different eID means. Having multiple eIDs results in the multiplication of the electronic identities of a citizen. Multiplicities of eIDs cause a burden for citizens, businesses and governments in the EU, while the goals of achieving a Digital Single Market are still unachievable. Also, many researchers acknowledged that the main challenges for pan-European electronic identity are, among other things, the interoperability and diversity of the eIDMS, different approaches concerning technology, organisation and regulations on identity management (Andrade, 2012b; Andrade, Chen-Wilson, Argles, Wills, & Di Schiano Zenise, 2014; de Andrade et al., 2013; Kubicek & Noack, 2010; Melin, Axelsson, & Söderström, 2016b). The research on eID usually addresses the design and implementation for the national use with the meagre interest of the cross-border eID. The research on eID state of the art shows that researchers are mainly addressing technical and legal challenges for interoperable eID EU (Andrade et al., 2014; Bender, 2015; Brugger, Fraefel, & Riedl, 2014; Carretero, Izquierdo-Moreno, Vasile-Cabezas, & Garcia-Blas, 2018; Kamelia Stefanova & Dorina Kabakchieva and Roumen Nikolov, 2010; Myhr, 2008; Schweighofer & Hötzendorfer, 2013). Moreover, Whitley, Gal, and Kjaergaard (2014) acknowledge a lack of research exploring the interplay of policy, technology, and management of the eID in the organisational context. Furthermore, Melin et al. (2016b) emphasise the need for more research, among other things, on the national differences and governance structures of eID design and implementation (Melin et al., 2016b, p. 19).

Thus, this research explores the factors that affect the enactment of the cross-border digital identity in the EU from a national perspective. Exploration and identification of the factors that affect the enactment of the cross-border digital identity in the EU are necessary to inform policy makers and researchers of the existing factors that affect the mutual recognition of the eID in the EU. Furthermore, this research explores the opinion and perspectives on the new European Digital Identity Wallet, proposed by European Commission.

Finally, the purpose of this research is to explore the factors that affect the enactment of the cross-border eID in the EU from a national perspective. In addition, the objective is to provide recommendations on how to overcome the main challenges that affect the enactment of cross-border eID. Furthermore, this research aims to present the main commonalities and differences of identified factors affecting the cross-border eID enactment in case study countries. Hence, the main research question that this research tries to explore is: **“What factors affect the cross-border eID enactment in the EU**

from Estonian and Belgian perspectives?” In line with the central question and the purpose of this research, the following subquestions are addressed:

- What are the perspectives of Belgium and Estonia on the new eIDAS proposal and European Digital Identity?
- What are the recommendations to overcome identified challenges?

To answer the proposed research questions, this research is structured as follows. Firstly, in the following section, the theoretical framework and literature review are discussed and presented. Then, the policy background on the cross-border settings and eID field is presented and discussed as an essential background of EU eID initiatives to understand this research better. Methodology and research design are explained and discussed in the fourth section of this research. Furthermore, in the fifth section, the case study countries, implementation of the eID cards in the national context by Belgium and Estonia is explained. In the sixth section, findings and results gathered through data collection and analysis are presented and explained. Discussion of the gathered results and findings, comparison of Belgium and Estonian case, with recommendations on overcoming existing challenges, are presented in chapter six. Finally, in chapter seven, the author provides a summary of the research and answers to research questions.

2 Theoretical framework and literature review

Researchers emphasise that there is a need for further research on eID from an organisational perspective and considering eID as a technology (Whitley et al., 2014). In this research, eID is considered as a technology that is enacted in the government to enable online identification and authentication of citizens. Considering the need for further research on eID from the organisational and institutional perspective (Hedström, Wihlborg, Gustafsson, & Söderström, 2015; Melin, Axelsson, & Söderström, 2016a), the selected framework for analysis of the factors (in terms of drivers and challenges) for this research is Technology Enactment Framework (TEF) (Fountain, 2001, 2004, 2008). The enactment often refers to the process of actors' decision and tendency to implement specific ICT policies or technology to strengthen, improve, or reproduce existing practices in the public sector (Fountain, 2004). Hence, the research objectives are to explore and identify the factors that affect the enactment of cross-border eID in Estonia and Belgium.

The use of TEF helps to analyse and recognize the complex relations between the eID as information technology and the social structures, organisational, institutional and other external factors (Gil-Garcia, 2012). Furthermore, the use of TEF is helpful for practical reasons as it helps public managers to plan, design and implement the egovernment initiatives (Gil-Garcia, 2012), in this case, the enacting of the cross-border eID. It is developed as a result of the extensive research of the decision-makers in government and their design and use of ICTs (Fountain, 2004, p. 9).

2.1 Technology enactment framework as a theoretical framework

The purpose of this framework is to ensure the understandings and exploration of the information-based changes in governments (Fountain, 2004, p. 4). Many researchers have found that implementation of the information technologies in governments might lead to different results of the ICT implementation due to different organisational contexts (Fountain, 2004, p. 7). Fountain (2001) argues that one of the reasons was that the research on the effects of information systems in governments needs to consider the interrelations between organisations, key actors, and information technologies. Fountain (2001) argues that information technologies are enacted in governments by the key actors who are influenced by their interpretation, design, implementation and use of the information technologies in their organisation and networks (Fountain, 2001, p. 89). Hence, it is essential to analyse and consider the existing organisational processes, stakeholders, institutions, culture, and organisational change to understand and influence the implementation and use of the specific IT (Fountain, 2004, p. 5). The value of this framework lies in emphasising the importance and influence of the existing socio-structural mechanisms in the organisations and institutions, which helps public managers understand the design, development, implementation, and use of the new information system (Fountain, 2001, p. 89). To achieve this objective, the Technology Enactment Framework "integrates information technology into organization theory and extends related research programs on institutions, social networks, and embeddedness in sociology, economics, and political science to better account for the behaviour of bureaucrats in government agencies" (Fountain, 2001, p. 83). Furthermore, Fountain (2001) states that this framework explains the way how do the key actors in the institutions enact new information systems in order to reproduce the existing "to reproduce existing rules, routines, norms, and power relations in the institutions" (Fountain, 2001, p. 89). Consequently, Fountain (2001) states that technology enactment results from cultural, cognitive, structural and political embeddedness.

The analytical elements of the Technology Enactment Framework are organisational forms, institutional arrangements, actors, enacted technology and outcomes. For the purposes of understanding the TEF, the description of all elements of the framework is following.

Technological dimension

The most important distinction that is needed to be understood is between the "Objective Information Technologies" and "Enacted Technology" (Fountain, 2004, p. 9). Objective information technology includes hardware, software, IoT, Internet, and other technical systems (Fountain, 2001, p. 98). These objective technologies (technological factors) are, according to Fountain (2001), of little value until a knowledgeable person starts using them. For instance, internet protocols, authentication methods, mobile phones and other eID credentials are considered objective technology. Consequently, Fountain (2001) defines "enacted technology" as the perception, implementation and use of these objective technologies. However, the perception, use, design and implementation of these objective technologies are mediated by the context addressed in organisational forms (organisational factors).

Organisational dimension

Fountain (2001) classifies two organisational forms, bureaucratic and network forms. The bureaucratic form includes the logic of the hierarchy, standardisation, rules and control, which influences the decisions of the key actors when it comes to the implementation and use of the ICT. This can be altered, nonetheless, with the other organisational form, networks. Jointly with the bureaucratic form, the government is also involved in cooperation and collaboration with other government entities and other social actors. Conversely to bureaucratic form, the network form and interrelations between the entities is based on the informal rules, trust and social capital. Fountain (2001) also mentions that the networks are more effective where there is higher trust, social capital and where information is shared among the actors (Danziger, 2004, pp. 102–103). However, although networks can improve efficiency and effectiveness, they might also be the source of conflict and disruption (Danziger, 2004, pp. 102–103).

Institutional factors

The implementation, use and design of the ICT undergird the institutional arrangements (institutional factors). Institutions are stable practices, norms, values and processes that simplify or order behaviour of the actors (Fountain, 2008) "as "reproduced practices" that are both flexible and remarkably stable." (Fountain, 2001, p. 94)". Because all organisations function in a complex environment influenced by regulations and political decisions, the behaviour of the decision-makers is influenced by the cognitive, cultural, socio-structural and legal institutions (Fountain, 2001, p. 93). Cognitive institutions are the mental habits that influence the behaviour and decision making; cultural institutions refers to the symbols, narratives, meanings and other elements that constitute culture; socio-structural institutions are the social and professional networked relationships that enable and constrain the behaviour of decision-makers; and legal institutions are the laws and regulations that enable and constrain problem-solving and decision making (Fountain, 2004, p. 11).

Actors

Lastly but not least, Fountain (2004) describes three groups of actors which are involved in the technology enactment. The first group of actors are the vendors and consultants responsible for objective technology; their expertise lies in the technical understandings of the requirements and requests system. The second group of actors include the decision-makers and chief information officers in government; these actors bear most responsibility for the system design. Lastly, the third group of actors comprises the policy makers, managers, and administrators who have a strong influence, which is usually neglected on all elements of the technology enactment framework.

Outcomes

As the last element in this framework, outcomes are considered the impacts of the chosen and enacted information technology. These outcomes are influenced by the key actors' decisions, which are influenced by the organisational forms and institutional arrangements; therefore, they are "multiple, unpredictable, and indeterminate" (Fountain, 2001, p. 98). The relation between these elements is mostly recursive. This means the influence or causal connection flow. For instance, the institutional arrangements influence the organisational forms; however, organisational forms also might influence the change in the institutional arrangements (Fountain, 2004, p. 11). This recursiveness shows the uncertainty of the outcomes when the implementation, design and use of ICT are made (please see Figure 1).

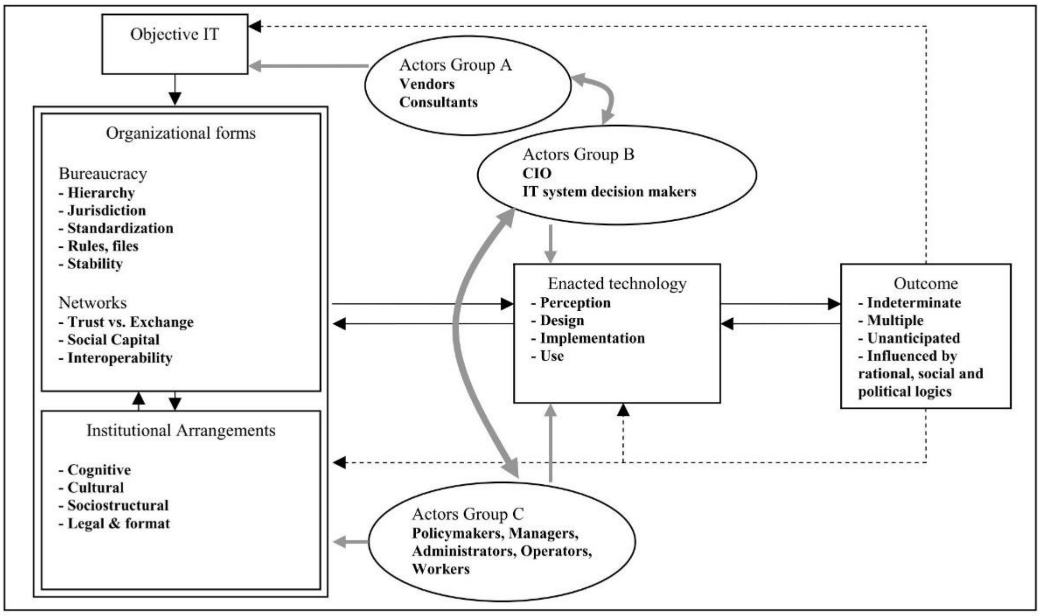


Figure 1: The Technology Enactment Framework (Schellong, 2004, p. 6)

The explained TEF is valuable for structuring the array of factors (Leosk, Põder, Schmidt, Kalvet, & Krimmer, 2021). Due to the specific research topic, scope and goals, this research's chosen analytical elements and dimensions are *institutional factors, organisational factors, and technological factors*. The choice of these elements lies in the research need to analyse the identified factors that affect the enactment of the cross-border eID from a national perspective. It is important to note that Fountain (2001) emphasise that these factors can either be a barrier to the enacted technology or a driver to enacting the technology.

2.2 Literature review

Identity and Digital Identity

There has been a discussion about electronic identity since the Internet became publicly available. Identity is a very complex concept including different types of identity and is very difficult to define (Andrade et al., 2014). For instance, there could be a national identity, whether Belgian, Estonian or Serbian, or mathematical identity of equations 3 = 2 + 1 (Andrade et al., 2014). Identity can be seen as the unique existence of a single, discrete, individual person, with various attributes that differentiate that individual from others in the group.

Following the explanation of identity, there is a slight distinction between identity in real life and online identity. The difference is that people usually have one public identity in real life, that they can decide whether to identify or not while using services (for instance, while using public transport). In contrast, in the online sphere, people are usually needed to identify themselves to use services (such as email, Facebook, public online services), but they are able to choose many identities and create their own identity, fake or real (Kubicek, 2010). Moreover, the difference is that in online situations identifying party is not another person but a computer or some technological system (Andrade et al., 2014).

Following the development of electronic government and that more public services are becoming online public services, citizens need to identify themselves to be able to qualify for benefits or services (Kubicek, 2010). Similar to the real identity, electronic identity is also built from various attributes, and usually, countries are using the same attributes from real-life identity data in eID means. Therefore, in this research, the concept of identity that is used is "one individual whose collection of main attributes differentiate from other individuals". Important elements and concepts of the electronic identity are its phases of use. These phases are, *inter alia*, electronic identification, electronic authentication and electronic authorisation.

Electronic identification is the process of using the attributes of a person to derive whom the person is claiming to be (Kubicek, 2010). In the eIDAS regulation, electronic identification means "the process of using person identification data in an electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person" (European Union, 2014, p. 83). Examples of identification in real life are the process of presenting to the respective party the standard set of data such as name, surname, birth date, address and unique personal identifiers.

Next to the identification is the concept of authentication. Authentication is considered the process of confirming the claimed set of attributes or facts with some degree of confidence (Kubicek, 2010). Furthermore, authentication in eIDAS regulation is defined as the "electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in the electronic form to be confirmed" (European Union, 2014, p. 84). There are several characteristics of authentication. The first one is the level of authentication, and it can be complete or partial authentication. Complete authentication is when the person identifies itself with all attributes (i.e., name, surname, address, citizenship), while partial is when the person identifies itself only with partial attributes (i.e., age). Shortly, authentication means to answer the question "Are you the one whom you claim to be?” (World Bank Group, 2016, p. 11). There are four most common factors or questions to enable full authentication or confirm whether the person is the one who claims to be. These factors and questions are: “What a person is?”, “What a person knows?”, “What a person has?”, “What a person does?” (World Bank Group, 2016). For example, the answer to the first question is whether the person is a citizen of the MS A or MS B, legal or natural person; the answer to the second question is whether a person knows the password or required PIN code; the answer to the third question whether a person has the smart card and the card reader; finally, the answer to the fourth question is person behaviour visually confirmed.

Finally, the last element of the electronic identity is an authorisation. Authorisation usually means the permission of authenticated identity to perform the action or use the wanted service (Kubicek, 2010). Authorisation can also be understood as permission to use or access. Also, that process is always on the service provider's side, which identifies and authenticates the person online and provides the requested service. For instance, buying online alcohol can be allowed only to people to a certain age threshold, and it can alcohol can be provided only if this requirement is fulfilled. If this is not the case, a person requiring that service will not be authorised or permitted to buy alcohol.

eID management systems

The identity management systems (IDMS) are defined as “identity management is the managing of partial identities of entities, i.e., definition, designation and administration of identity attributes as well as the choice of the partial identity to be (re-) used in a specific context.” (Kubicek, 2010, p. 13).

Identity management systems are crucial for creating, verifying and certifying electronic identities, with an overall objective to create confidence and trust between citizens and service providers (Andrade et al., 2014). Andrade et al. (2014) state that there are two sides of IDMS, the user side and the administration side. On the user side, IDMS should allow access to services for relevant people and manage their identities as some attributes change over time (after marriage, the surname is changed). While on the administration side, which is the focus of this research, IDMS are the processes in which “organizations, businesses, companies, and institutions grant, control, and manage user access to information, applications, and services over a wide range of network services” (Andrade et al., 2014, p. 6).

Electronic identification management systems (eIDMS) have similar elements as in the regular IDMS. The main difference is that identification, authentication, and authorisation always happens digitally and almost always online on the internet. For the purposes of this research, eIDMS are usually perceived as institutions and actors that aim to solve existing problems in cross-border settings and that are results of strategic interactions between the actors (Kubicek, 2010, p. 17). The importance of the eIDMS is because the proper management of the eID establishes trust and higher confidence among remote interactions of the organisations or individuals (OECD, 2011a, 2011b). Furthermore, the eIDMS is perceived as the critical enabler for egovernment services that should be developed before designing and planning electronic services (Aichholzer & Strauß, 2010).

In the eIDAS regulation, the system and processes of issuance of the eID are defined as the electronic identification scheme. This eID scheme is defined as “a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons” (European Union, 2014, p. 83).

In eIDMS, several stakeholders are involved in managing electronic identities. Main stakeholders involved in eIDMS are the public sector, private sector, enabling and supporting actors and end-users. All these stakeholders have a specific role in eIDMS. These roles, *inter alia*, are identity providers, service providers, end-users and attribute providers (CEF Digital, n.dd).

Identity providers are the institutions or organisations that issue the electronic identification means and attributes to the natural or legal persons (eID card) (CEF Digital, n.dd). Also, identity providers provide authentication, authorisation and issue assertions (Carretero et al., 2018).

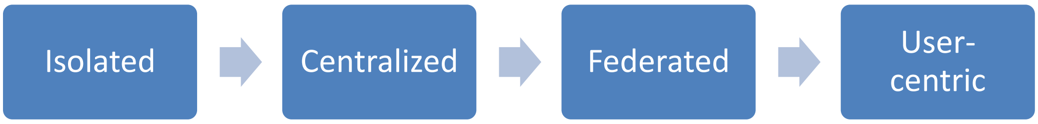
Service providers are usually public or private organisations that provide specific online services to the respective natural or legal person. These service providers usually rely on the identity providers on the identity provider by using assertions issued by the identity provider (Carretero et al., 2018).

Attribute providers are organisations or entities that are entitled to manage specific information and attributes about respective natural or legal persons. End-users are organisations, citizens or any entities using services on the internet and are required to identify.

It is important to note that in some models of eIDMS, any stakeholder can have multiple roles. For example, a specific public sector entity can be at the same time identity provider and service provider. These stakeholders with specific utilized roles are involved in the eIDMS ecosystem and thus specific eIDMS model.

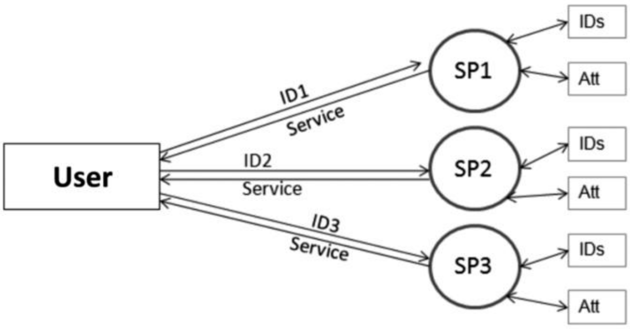
Currently, among scholars and practitioners, there are common understandings and acceptance towards four main categories of existing eIDMS models. These models are usually categorised into the four main categories: isolated, centralized, federated and decentralized/user-centric (Ribeiro, Leitold, Esposito, & Mitzam, 2018). Furthermore, according to Pöhn and Hommel (2020), the evolution of these models is usually perceived as the linear process, as can be seen in Figure 2.

Figure 2 eIDMS models evolution (Pöhn & Hommel, 2020).



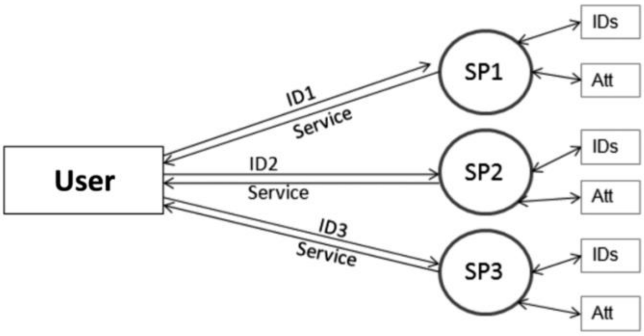
The isolated model of the eIDMS usually assumes that one entity or organisation acts as the service provider and identity provider simultaneously (Angelis, Falcioni, Ippoliti, Marcantoni, & Rilli, 2016). This means that there is one entity that controls all four processes of electronic identification, as mentioned above. This model was primarily utilised in the early stages of internet use because it is simple to implement. However, with the further development of the digital society and the growth of online services, this model showed some drawbacks (Angelis et al., 2016). Figure 3 presents the isolated model with figure created by Laurent, Denouël, Levallois-Barth, and Waelbroeck (2015)

Figure 3 Isolated model (Laurent et al., 2015, p. 34)



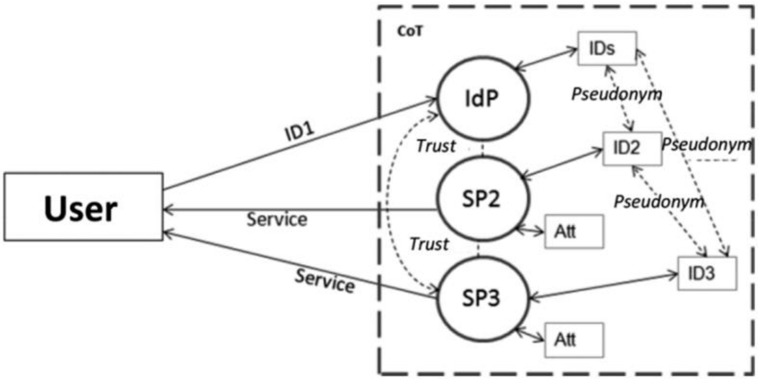
On the other hand, the centralised model is used to overcome the challenges imposed with the isolated model. Unlike the isolated model, this centralized model separates the roles of the service provider and identity provider (Angelis et al., 2016). There is one identity provider that keeps all identities and stores data about those entities and providing it to different service providers. Thus, this separation is suitable for managing many identities and users of service providers (Angelis et al., 2016). For example, this model is most commonly used and can be seen on the internet. The Single Sign-on service offered by platforms such as Facebook and Google is an example of a centralised model that can be accessed to various services such as, *inter alia*, on Facebook, Instagram or Youtube. However, although it overcame the challenges and risks of the isolated model, it has an important disadvantage: all identities are stored and controlled by one entity (Angelis et al., 2016). Thus, it contains one single point of failure, which is an identity provider (Carretero et al., 2018).

Figure 4 Centralized identity management model (Laurent et al., 2015, p. 35)



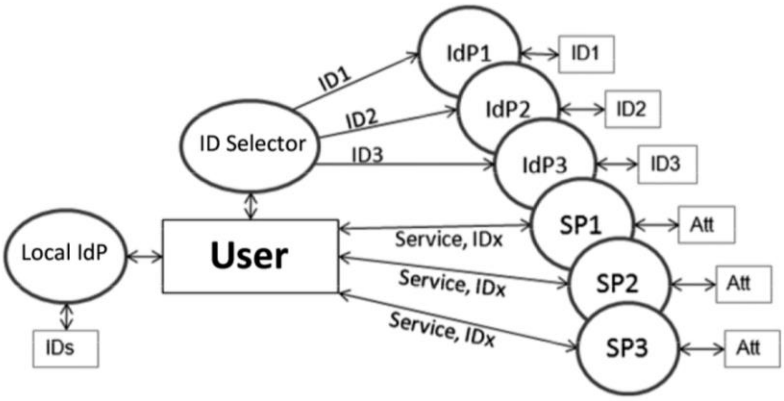
The federated model (Figure 5) contains many entities acting separately as identity providers and service providers (Angelis et al., 2016). This is enabled by agreed protocols, standards and trust frameworks among the service providers and identity providers. Thus, the user can use different identification methods to identify and authenticate for one specific person. However, one of the disadvantages is that there should be an agreed framework that supports the interconnection between service providers and identity providers. Currently, enabling electronic identification across the EU with different identity providers, this federated model is mostly used and perceived as the best solution for cross-border eID (Carretero et al., 2018).

Figure 5 Federated identity management model (Laurent et al., 2015, p. 36).



Finally, the user-centric management model usually means when the end-users control the management and sharing of their information and attributes (M. Lips, 2008). Very often, this user-centric model is also considered as a self-sovereign identity model (SSI). However, one of the disadvantages of this model is that users should accept the responsibility of informational privacy; hence, no organisation can guarantee protection for them (M. Lips, 2008). Thus, some scholars and practitioners perceive the user-centric model to be more susceptible to crime (M. Lips, 2008, p. 22).

Figure 6 User-centric identity management model (Laurent et al., 2015, p. 37)



Cross-border eID in the EU

Mutual recognition of the eID raises many challenges (Andrasko, 2017). Currently, not all MS have developed the eID solutions, and also, some who have eID have not notified EC according to eIDAS regulation.

There are several causes for the lack of interoperability in the eID field in the EU. The existing diversity of approaches towards the design and implementation of eIDMS is one cause. For example, some countries in the EU, such as Belgium and Estonia, adopted a federated identity management model, while some countries, such as Germany, adopted a centralized approach (Shehu et al., 2019). Consequently, different approaches of eIDM systems led to different rules towards eID, varying from the use of Public Key Infrastructure (PKI) to reliance on a two-factor authentication system (Andrade, 2012b).

In addition, different approaches toward unique personal identifiers are identified as one of the main challenges for achieving interoperable eID across borders (Aavik & Krimmer, 2016; Hinsberg et al., 2020; S. Lips, Bharosa, & Draheim, 2020). Unique personal identifiers are issued data by the government from which citizens or businesses can be uniquely identified for identification and authentication purposes. Hence, approaches towards unique personal identifier in EU is quite different. For example, in some MS, unique personal identifiers are mandatory, such as in Estonia and Belgium, while in some countries, it is constitutionally illegal to have unique personal identifiers, such as in Germany and Hungary (Shehu et al., 2019). The different approaches lead to challenges for cross-border access to procedures. Mainly, when national electronic services were design and implemented in MS, the main goal was to offer access to nationals of that MS. Consequently, service providers who offer services in one MS do not recognise other unique personal identifiers from other MS. Hence, causing the inability for identification and authentication by citizens and business from different MS. To overcome this obstacle, nationals from other countries must apply for a resident ID or obtain other eID mean (i.e. BankID)o access the procedures (Hinsberg et al., 2020). Thus, the motivation to use national state-issued eID for cross-border services in accordance with eIDAS regulation remains low, according to Hinsberg et al. (2020). This situation leads a citizen to obtain many different eID means with different unique personal identifiers, which for the electronic systems means that it is two different entities, so-called “Digital Twins”. For the purposes of identification by public administration, the challenge with the lack of EU unique personal identifiers lead to identity matching. Identity Matching is the correct authentication of an entity with given attributes and assurance that that entity is who he/she claims to be. Furthermore, S. Lips et al. (2020) emphasises that the most challenges are related to cross-border e-service provision rather than eIDAS implementation in the countries themselves.

The technological architecture and infrastructure that is developed and in use for the cross-border eID in the EU are primarily based on the results and successes of the three main large scale projects in the EU (Cuijpers & Schroers, 2014). These projects are STORK[3], STORK 2.0, eSENS (Cuijpers & Schroers, 2014). In this research, only STORK and STORK 2.0 projects are described due to the relevance of their results for the cross-border eID in the eIDAS regulation.

The first version of the STORK project started in May 2008 and lasted until 2012, with the objective to develop an interoperability framework to enable cross-border mutual recognition of national eID (Leitold Herbert & Posch Reinhard, 2012). In total, this project involved 18 EU and EEA states[4]. Through this project, conceptual interoperability models and quality authentication assurance acting as the basis for trust framework were developed (Leitold Herbert & Posch Reinhard, 2012). Furthermore, it is important to note that this quality authentication assurance acts as the basis and foundation for the level of assurances in the eIDAS regulation. The STORK large scale projects focused on six main

[3] Stork is abbreviation of the “Secure Identity Across Borders Linked”.

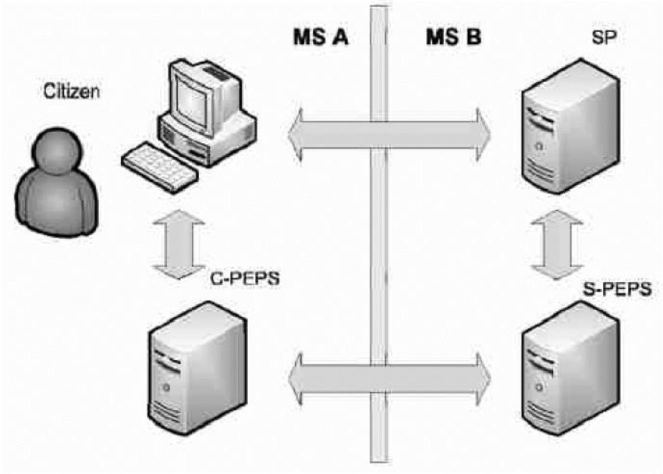
[4] States that were involved are: Austria, Belgium, Estonia, France, Germany, Iceland, Italy, Luxemburg, Portugal, Slovenia, Spain, Sweden, The Netherlands, and United Kingdom Finland, Greece, Lithuania, and Slovak Republic.

pilots. The first pilot was “Cross-Border Authentication Platform for Electronic Services”, the second pilot was “Safer Chat pilot”, the third pilot was “Student Mobility”, the fourth pilot was “Electronic Delivery”, the fifth pilot was “Change Address pilot”, and finally, the six pilot was on “The European Commission Authentication Service”.

STORK developed two approaches for the interoperability model and technical solutions that enable the mutual recognition of cross-border eID. These approaches differ based on the eIDMS in the countries, whether it is centralized, having one central gateway enabling authentication, or decentralized with several gateways for authentication.

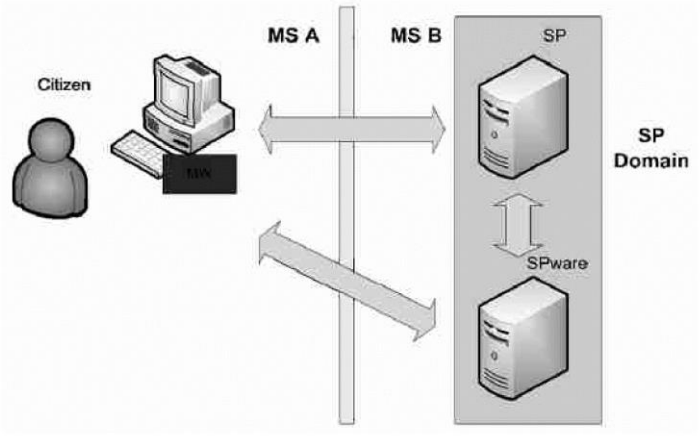
In cases where MS uses a centralized gateway for authentication and e-services, STORK developed Pan-European Proxy Service (PEPS), enabling authentication between MS (see Figure 7).

Figure 7 Solution for centralized gateway approach PEPS (Leitold Herbert & Posch Reinhard, 2012, p. 296)



The other solution that STORK developed is for the MS with a decentralized approach for authentication of its citizens. Usually, decentralized systems are developed when there was a need to overcome legacy systems in order to enable interoperability of those separated systems. Thus, STORK uses a middleware solution that decouples the legacy service and transforms the protocol, which enables interoperability (Leitold Herbert & Posch Reinhard, 2012). In this case, there is no need for additional centralized infrastructure; however, middleware needs to be incorporate the national protocols that use different eIDs (Leitold Herbert & Posch Reinhard, 2012, p. 297).

Figure 8 Solution for decentralized approach (Leitold Herbert & Posch Reinhard, 2012, p. 297)



Following the successful results of the first STORK project, STORK 2 was initiated to continue developing interoperability of the national eID schemes across borders. The main differences between the STORK and STORK 2.0 are pilots that were implemented to enable interoperability. Main pilots in STORK 2.0 were the “eLearning and Academic Qualifications”, “eBanking”, “Public Services for Business and eHealth areas”.

The results of the STORK and STORK 2.0 project showed that it is possible to have technically enabled mutual recognition of the eIDs in the EU for cross-border settings. Interoperable and mutually recognized eIDs in the EU can have several benefits for different actors, according to Servida (Servida, 2019). These benefits are, *among other things*, ease of use, cost savings, increased assurance, and new application areas.

3 Policy background and the cross-border context in the EU

This section describes the policy background of the EU on enabling the cross-border digital identity. Also, one of the EU's main goals is to achieve and establish a Digital Single Market for citizens and businesses. Policies developed in the last 20 years in the EU assert the precise objectives of the EU and MS towards seamless cross-border service provision. Firstly, the most relevant policies related to the cross-border services provision and objectives are described. Secondly, the EU's initiatives towards the development of interoperability in the EU and its programmes are described. Thirdly, the policy context related to the development of eID in the EU is described and explained. Thus, this section provides a clear description and enables an understanding of the EU past and future goals in cross-border integration, service provision and interoperability governance of the eID.

3.1 Cross-border services policy initiatives

EU Service Directive 2016/123/EC

In order to enhance EU integration and improve administrative simplification, the EU has addressed the opportunities and challenges of the cross-border services by adopting the Directive on services in the internal market (EU Service Directive) (Directive 2006/123/EC, 2006). The EU Service Directive is considered to have revolutionised effect on public services, as it is the first document by European Commission (EC) that establish the binding rules on administrative simplification (Hatzopoulos, 2008). The goals of this directive are to improve the service provision across borders and enable efficient access to information by businesses and citizens. Moreover, one of the main elements is the binding rule that all governments should establish a single point of access by 2009 (Hatzopoulos, 2008; OECD, 2020). Establishing the online platform was the prerequisite to improve access to information and procedures for cross border users. The findings of the assessment of the Single Point of Access platforms from 2015 emphasised a space for significant improvement in the accessibility for cross-border users (OECD, 2020). Furthermore, access to information and procedures from other MS is a considerable problem, more specifically, the availability to use of e-signatures and eID (OECD, 2020).

Malmo Ministerial Declaration on eGovernment

In 2009, when the EU Service Directive came in force, Ministers of the MS in the EU signed a Malmo Ministerial Declaration on eGovernment. Malmo declaration set the goals, priorities and commitment of MS in the egovernment field for 2015. In this declaration, MS committed to work on establishing improved digital cross-border services and promote a common culture of collaboration ("Malmo Ministerial Declaration on eGovernment," 2009). Furthermore, the importance of the seamless public cross-border services and mobility of the citizens and business is acknowledged as a priority. Identification of the gaps in cross-border interoperability and mutual recognition of the eIDs is set as one of the priorities in this declaration.

Digital Single Market Strategy

Acknowledging the challenges posed by the rapid development of the ICT and its influence in the society, EU decided to overcome these challenges and barriers by adopting "A Digital Single Market Strategy" (DSMS). The DSMS was launched in 2015 and was one of the main priorities of the Juncker Commission. Digital Single Market is defined as "one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence" (European Commission, 2015c, p. 3). The market benefit of the digital single market is accounted for an additional 415 billion EUR to European GDP (European Commission, 2015b). To overcome the challenges and barriers hindering the creation of the digital single market, the DSMS is built on three pillars. The first pillar is about enabling citizens and businesses to access online goods and services. This would require extensive work on removing differences in the online and offline world. The second pillar is about creating fair and the right conditions for digital businesses and services to develop. This would require the development of interoperable digital infrastructures and content services. Finally, the third pillar is maximising the growth potential of the European Digital Economy. This pillar is the most relevant for the digital government field. Therefore, the EU called for the development of interoperable solutions and a new eGovernment action plan with the inclusion of the once-only principle and mandatory interconnection of base registries.

Tallinn Declaration on eGovernment

Building on the achievements of the Malmo Declaration and priorities and goals set by the DSMS, Ministers of EU and EFTA countries signed the Tallinn Declaration on eGovernment in 2017 ("Tallinn Declaration on eGovernment," 2017). The Tallinn Declaration sets the priorities of the signatories towards the development of high quality, user-centric public services and seamless cross-border services for citizens and businesses (European Commission, 2017). The vision emphasised in the Tallinn declaration states that signatories will "strive to be open, efficient and inclusive, providing borderless, interoperable, personalised, user-friendly, end-to-end digital public services to all citizens and businesses – at all levels of public administration." ("Tallinn Declaration on eGovernment," 2017, p. 3). Important innovation from the Malmo declaration is the recognition of the six leading principles for the design and implementation of the eGovernment policies in order to achieve set objectives. The principles that are guiding the development of the e-services in the EU by this declaration are: Digital-by-default, inclusiveness and accessibility; Once only principle; Trustworthiness and Security; Openness and transparency; Interoperability by default; Horizontal enabling policy steps ("Tallinn Declaration on eGovernment," 2017).

Single Digital Gateway Regulation 2018/1724

Building on the establishment of the Single Points of Access from the Service Directive, the EU has adopted the Single Digital Gateway Regulation in 2018 (Single Digital Gateway Regulation, 2018). According to the findings of the lack of clear provision of information and access to procedures by the cross-border users, the EU aimed to create one single platform or single digital gateway (SDG) for all citizens of the EU. With this regulation, the EU aims to enhance access to information and procedures by all EU citizens through creating a single digital gateway (SDG). The Single Digital Gateway will enable citizens across the EU to provide feedback and access to information and procedures on the "Your Europe Platform". More specifically, the MS are required to share data, information and documents among themselves to ensure proper implementation of the single digital gateway and to ensure access to procedures by the cross-border users. Furthermore, in Article 13 of the Regulation (2018/1724), it is stated that MS need to ensure that all procedures which can be „accessed completely online by non-cross-border users, it can also be accessed and completed online by cross-border users in a non-discriminatory way by means of the same or an alternative technical solution procedures" (Single Digital Gateway Regulation, 2018). Single Digital Gateway should come into full operation in 2023, which means that eID mutual recognition should be applicable in cross border situations, while cross-border once-only principle should be fully adopted among MS in the EU.

Berlin Declaration

Building on the success of the Malmo Declaration and Tallin Declaration, which marked a milestone for service-oriented, innovative and reliable egovernment in Europe, EU officials and Chief Information Officers (CIOs) of MS signed a "Berlin Declaration on Digital Society and Value-Based Digital Government" ("Berlin Declaration on Digital Society and Value-Based Digital Government," 2020). Berlin Declaration reassures political commitment towards the value-based creation of the digital government and digital public services. Signatories acknowledged the importance of the public sector as an essential element for European Single Market, hence agreed on the focus on several policy action areas. Signatories of the Berlin Declaration agreed, *inter alia*, to promote the rollout and use of eIDs and introduce incentives for the private sector in the field of eID. Furthermore, the EU institutions are called to continue developing the EU-wide

Digital Identity framework, which will enable more cross-border transactions and improve Digital Single Market. Finally, signatories agreed to continue implementing the SDGR, with a specific focus on "fostering interoperability by the design of policies, data, solutions and services to enhance cross-border and cross-sector interconnections" ("Berlin Declaration on Digital Society and Value-Based Digital Government," 2020).

Shaping Europe's Future

EC commission adopted a communication, "Shaping Europe's Future", which lays down the vision for the 2020-2025 period on harnessing the potential of digital transformation based on human value-centric principles (European Commission, 2020a). Through this communication, EC committed to working on the three key priority objectives, ensuring fair digital transformation that works for the benefit of the citizens and businesses (European Commission, 2020a). The first objective is to work towards the "Technology that works for people". The second objective is to work towards "A fair and competitive economy". Last but not least, the third objective is to work towards "An open, democratic and sustainable society". Through the third objective, it is acknowledged that the universally accepted eID across the EU is necessary to build trust for the interaction of citizens and businesses across the EU. Hence, one of the key actions that EC will commit to in the next five years is to work on improving the current eID state of the art and extend its benefits to the private sector and promote eIDs for all Europeans (European Commission, 2020a, p. 12). In addition, EC committed to work on reinforcing EU governments interoperability strategies in order to ensure coordination and cooperation for secure and borderless public sector services (European Commission, 2020a, p. 7).

This description of the policies is related to the development of the cross-border provision of public services and interoperability. It can be acknowledged that EU institutions and MS are committed to cooperate and work on the creation of the Digital Single Market in the EU. Moreover, cross-border recognition of eID has been acknowledged that presents a challenge towards the achievement of the Digital Single Market. Hence, the EU has recognised the importance of the eID as a key enabler for the provision of digital public services and eGovernment in general.

3.2 EU interoperability governance

EU has been aiming to achieve interoperability in public services across sectors since 1995. The first programme, the electronic interchange of data between administrations ('IDA programme'), was created for the period 1995-1999. The main objective of the IDA programme was to achieve high interoperability of telematic networks for data exchange in public administrations (European Commission, n.db). Furthermore, the aim was to extend the achievements of this programme to citizens and businesses. Areas that the IDA programme was addressing was in Economic and Monetary Union, consumer protection, health and transport (European Commission, n.db). After successful achievements, the successor of IDA, the IDA II programme, continued work on the interoperability of public administrations for the period of 1999-2005. IDA II's goals were extended not only to enable interchange data between public administrations but also to increase efficiency at the pan-European level (European Commission, 2005). Furthermore, in 2002 EC adopted revisions of the IDA II programme, which for the first time included references to identification and deployment of the cross-border digital public services for citizens and businesses (European Commission, 2005, p. 1). Additionally, within this programme, the 'Your Europe' platform was created, which will now serve as a single digital gateway based on SDGR.

The follow-up programme of both IDA programmes was the "interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens" (IDABC). IDABC was established for the period from 2005 to 2009. The objective of this programme was to support and enable MS to deliver interoperable cross-border public services (IDABC, 2007). With the development of ICTs, it is acknowledged that there is a need for further cooperation to overcome the constant challenges persisting in the development of the European Single Market and cross-border public sector services provision (IDABC, 2007). Additionally, the objectives from previous programmes IDA and IDA II was extended towards facilitating and achieving interoperability of cross-border public services across the EU ("The IDABC Programme (2005-2009)"), based on the first European Interoperability Framework created in 2004.

The follow-up programme of IDABC, the interoperability solutions for European public administrations (ISA programme and ISA^2) was in force in two terms, 2009-2015 (ISA) (ISA programme, 2009) and 2016-2020 (ISA^2) (ISA2 programme, 2015) in 2009 and operated until the end of 2020. The ISA programme has continued its predecessors' achievements and continued the coordination on the development of cross-border services and interoperability in the EU. Once again, it is acknowledged that there is a need for further coordination and a comprehensive approach towards the ICT solutions in MS (European Commission, n.d.a). Without this coordination and comprehensive approach, MS will continue developing incompatible solutions which might hinder the process of creating a Digital Single Market, hence create a barrier for access to procedures and information across borders. Within the ISA and ISA^2 programme, the European Interoperability Framework importance is acknowledged, which act as a guideline document for developing interoperable solutions and policies. ISA^2 programme has several achievements in the field of interoperability. According to the Interim Evaluation of the ISA^2 programme (CEPS, 2019), the programme is highly significant and relevant for achieving interoperable cross-border services across the EU. Within this programme, interoperable solutions were developed which enables interoperability in the EU. Finally, one of the most significant achievements of the ISA^2 programme is increased awareness of interoperability value and benefits for public administrations, businesses and citizens in the EU (CEPS, 2019).

In addition to the interoperability programmes initiated by the EC, there is also synergy and a high level of coherence with other EU programmes. For example, the Connecting Europe Facility (CEF) programme was established in 2013 to support cross-border interaction by developing the interoperable digital services infrastructure for cross-border use cases (CEF Programme, 2013). CEF Digital supports cross-border digital services by providing key building blocks or key enablers. The value of these building blocks is seen in reusability as they can be modified for specific use by MS if needed (CEF Digital, n.da). One of the most used building blocks of CEF Digital is the eID solution. CEF eID solution provides MS the digital infrastructure for electronic identification (eID) that is interoperable and that enables the mutual recognition of national eIDs (CEF Digital, n.d.b).

3.3 EU eID policy development

EU has been involved in regulating the e-communication services, such as electronic signatures (eSig), since 1999. The first legal document aiming to establish the utilization and issuance of eSig was the “eSignature Directive” (ESignature Directive 1999/93/EC, 1999). The main objective of the eSig Directive was to promote trust in digital communication and the digital environment (de Andrade et al., 2013). Furthermore, the aim was to create a legal framework that will enable the use of eSig within the internal market in the EU. The biggest achievement of the eSig Directive was the legal recognition of the eSig, which became legally equivalent with handwritten signatures (Dumortier & Vandezande, 2012). Hence, it is expected that the creation of the legal framework for eSig will boost e-commerce activity and enable trust among the parties involved.

However, the implementation of the eSig Directive faced many challenges (Andrade, 2012a, 2012b; Dumortier & Vandezande, 2012; Lentner & Parycek, 2016). Mainly, the European eSig market did not evolve due to interoperability issues (Lentner & Parycek, 2016). eSignature directive was not imposing any common standards of, in particular, no common standards for relations between different eSig providers. This led to the heterogenic development of eSig, which resulted in a lack of interoperability within the EU. Interoperability of eSig was considered poorly or was not considered at all, according to the report on “Cross-border Interoperability of eSignatures” (Sealed & time.lex and

Siemens, 2010). Important aspects of the lack of success of the eSignature directive, next to interoperability issues, are the lack of identity definition and how identity can be established in the electronic environment (de Andrade et al., 2013). The problem arose because the parties could not confirm the identity of the signature person. The main issue was that parties could not solve the issue of authentication and answer the question “who is the person I am communicating?” and also “am I sure that he/she is, whom he/she claims he/she is?” (De Andrade et al., 2013). The necessity to ensure the unique identity of signatory became more important with the public administration digitalisation and with the further development and use of social networks (Lentner & Parycek, 2016; Lusoli, Maghiros, & Bacigalupo, 2008). The low promotion of interoperability and lack of framework for identifying citizens and business-led MS to develop solutions and policies with a focus on national purposes.

With the existing heterogeneity of eSig infrastructure and the necessity for unique identification of citizens and business, EC acknowledged that the eSig directive had not been a major access (Dumortier & Vandezande, 2012). The milestone for developing a comprehensive framework and legitimising the EU involvement in the regulation of eID processes was the signing of the Treaty of Lisbon (Andrade, 2012a). In the Treaty of Lisbon, it is acknowledged for the first time the concept of EU citizenship and further emphasised the importance of the internal market (Andrade, 2012a). Furthermore, EC initiated several large-scale projects[5] focusing on solving challenges of cross-border mutual recognitions of eSig and eIDs. The EU has also initiated the so-called ’large scale projects’ to research and test the environment for successful development of the seamless online public services and aims to achieve cross-border eID from 2006 (Monfort, Krempels, Majchrzak, & Turk, 2016). For example, projects like STORK, STORK 2.0 and TOOPhowed that the use of national eID is possible in the cross border use cases and that also once-only principle is achievable (Carretero et al., 2018). This showed that technical interoperability can be achieved and that eIDMs are interoperable.

eIDAS Regulation

Hence, EC proposed and adopted in 2014, “Regulation on electronic identification and trust services for electronic transactions in the internal market” (European Union, 2014). This regulation appealed the eSig directive with the focus to solve challenges for eSig, eID and trust services. eIDAS regulation aims to enhance trust in electronic transactions for public administrations, citizens and businesses. This, on the other hand, will increase the usage and effectiveness of public and private online services (European Union, 2014).

[5] The projects focusing on creation of cross-border eID are “PRIME, FUTUREID, STORK, STORK 2.0”

eIDAS provides a comprehensive framework for cross-border and cross-sector electronic communication and interaction across the EU (de Andrade et al., 2013). Article 5 of the eIDAS regulation specifically determines that cross-border users should be enabled and allowed to access procedures without any discriminatory obstacles, wherever online service or procedure is offered (European Union, 2014). More specifically, all MS are incentivised to recognize and enable identification and authentication of citizens and businesses holding eID means from another MS (Delos et al., 2015).

The process of mutual recognition of eID is based on notification processes of eID schemes to EC, as described in Article 9 of the eIDAS regulation. Through the notification process, MS provide information about the eID scheme, level of assurance and issuer of that eID. The deadline to start the notification procedure is one year after the implementing act adopted by the EU. Thus, the notification process of the eID means by the MS is predefined and agreed in the EU act on Commission Implementing Decision 2015/1984 on notification procedures of eIDAS regulation.

Only notified eID schemes from the MS can be recognized across the EU; hence only those eIDs that are notified can be used across borders. Furthermore, it is important to acknowledge that the process of notification of eID schemes is on a voluntary basis, which means that decision to notify the existing MS eID scheme is on the MS.

The importance of the security of the eIDs in the EU has been addressed through the level of assurance in the eIDAS regulation. This regulation has proposed the common framework for security and assurance of the identity and eID schemes. Level of assurance refers to the level of certainty and confidence in the claimed identity of the natural person (CEF Digital, n.d.c). Based on the complexity of the issuance and authentication of the eIDs, three LoA are possible, according to the eIDAS regulation; Low, Substantial and High. To ensure security and interoperability of eID means, EC adopted the act on implementing decision 2015/1502, which sets minimum technical specifications and procedures for eID means notified by MS. With this decision, it is defined what constitutes the level of assurance of the eID means. Levels of assurance are based on the quality of the registration process and the quality of the electronic authentication process.

eIDs with the low assurance level is online registration with the email account and password, for example. Substantial level of assurance eIDs, requires verification of the identity information online, in addition to the process of low level of assurance. eIDs with the high level requires registering and issuing eID cards in person, with multiple factors for authentication (CEF Digital, n.d.c). Thus, one of the most secure and reliable confirmations of identity online is all eIDs issued with a high level of assurance.

EU adopted several acts on the implementing decisions for the eIDAS regulation by setting the frameworks for enabling the cross-border eID. In the case of technical requirements and technical implementation of eIDAS, this regulation has been acknowledged as technology-neutral. This means that there are no predefined technical requirements to be implemented by MS. However, to ensure interoperability across the EU, it is necessary to predefine existing standards, processes and frameworks to enable cross-border eID. To achieve interoperability across the EU, Commission adopted decision 2015/1501 on the interoperability framework for the eIDAS regulation.

With this act, it is defined what would be the processes of the cross-border electronic identification can be achieved. Interoperability of the cross-border eIDs is achieved through CEF eID Nodes. These nodes are a connection point through which is enabled cross-border authentication of the persons, hence, enabling MS A to recognize eID means of the MS B (European Commission, 2015a). There are two types of eID nodes, receiving nodes and sending nodes. Therefore, all MS are required to implement eIDAS nodes to enable cross-border authentication in the EU.

Furthermore, to enable interoperability of the eID means, mandatory data elements of the natural persons, which are transmitted to the affected e-services, are prescribed in the Annex of the Implementing decision 2015/1501 on the interoperability framework (Klimkó, Kiss, & Kiss, 2018). The minimum data sets addressed in the implementation (European Commission, 2015a) act are:

- *(a) current family name(s);*
- *(b) current first name(s);*
- *(c) date of birth and*
- *(d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time*

Proposed amendments on the eIDAS regulation – European Digital Identity Framework

On the 3rd June 2021, EC published a new eIDAS proposal for amending eIDAS regulation and establishing a framework for establishing European Digital Identity[6]. This proposal follows up on the statement of the president of EC Ursula von der Leyen, that soon all European should have one European digital identity (Ursula von der Leyen, 2020). Moreover, reasons for proposing new amendments to the eIDAS regulation are lack of notified eID schemes, emerging market trends, inherited limitations of the public sector and lack of support for private providers (European Commission, 2021b). To overcome existing challenges and barriers, EC proposed the creation of the Digital Identity Wallets based on the European Self-Sovereign Identity Framework (ESSIF). According to the Proposal, Digital Identity wallets are perceived as the most suitable solution for attribute sharing by the private and public stakeholders(European Commission, 2021b, p. 6). Thus, this proposal requires all MS to issue a European Digital Identity wallet under the notified eID schemes (European Commission, 2021b, p. 9). Furthermore, notification of at least one eID scheme is made mandatory to all MS of the EU (European Commission, 2021b, pp. 9–10). The issuance and notification of at least one eID scheme and European Digital Identity Wallet are required within 12 months after the entry into force of the new regulation on the EU eID (European Commission, 2021b, p. 23).

[6] Proposal for establishing the European Digital Identity Framework will be addressed as “Proposal”

4 Research design

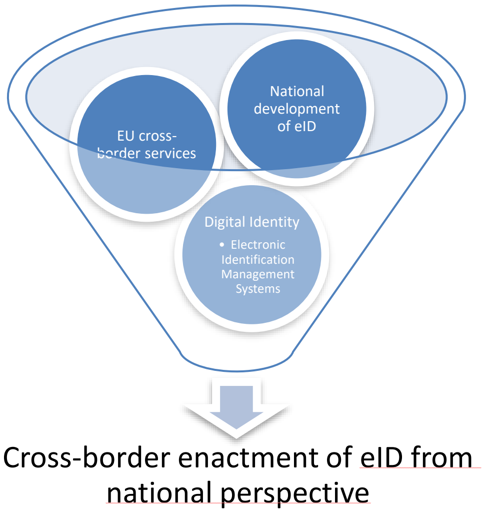
In this section, the procedures that are guiding this research are described. Saunders, Lewis, and Thornhill (2009) inspired the structure of this chapter and will guide the author throughout all stages of the research.

4.1 Research process

It is important to note that the research process conducted in this research was not linear but rather reiterated. Thus, since eID is a multifaceted technology (Kubicek, 2010), involving many dimensions like social, technological and legal, the research process of clear and robust definition of the research problem and research question has been mainly circular. However, the author follows the main questions in the research process which base a framework for research suggested by Walliman (2011). These main questions are "What is the subject of the research?" (what), "Why is this research relevant?" (why), "How is the research going to be done?" (how), and "When is this research conducted?" (when) (see Figure 11).

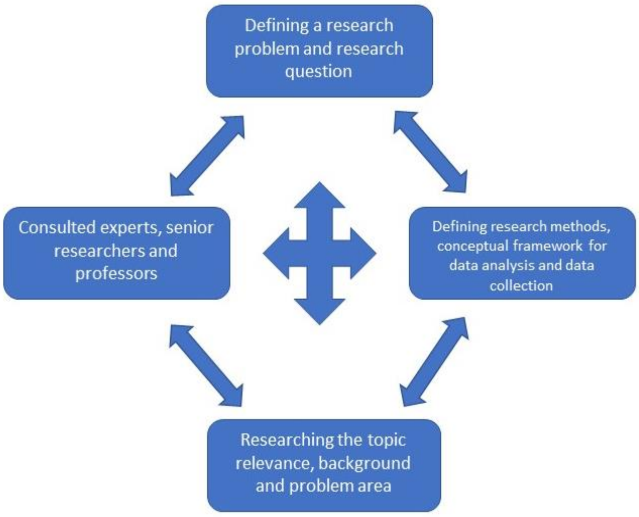
Firstly, at the beginning of the research, the author considered the main topics of interest for broad analysis. These topics are cross-border services, national development of the eID and digital identity. Considering the broad scope of the topics and the need for narrowing the research scope, question "what" is partly answered by reviewing the selected topics and integrating them into one research topic "cross-border enactment of eID from a national perspective". Figure 9 presents the topics reviewed and the final research subject.

Figure 9 Defining the subject of the research


National development of eID
EU cross-border services
Digital Identity
• Electronic Identification Management Systems
Cross-border enactment of eID from national perspective

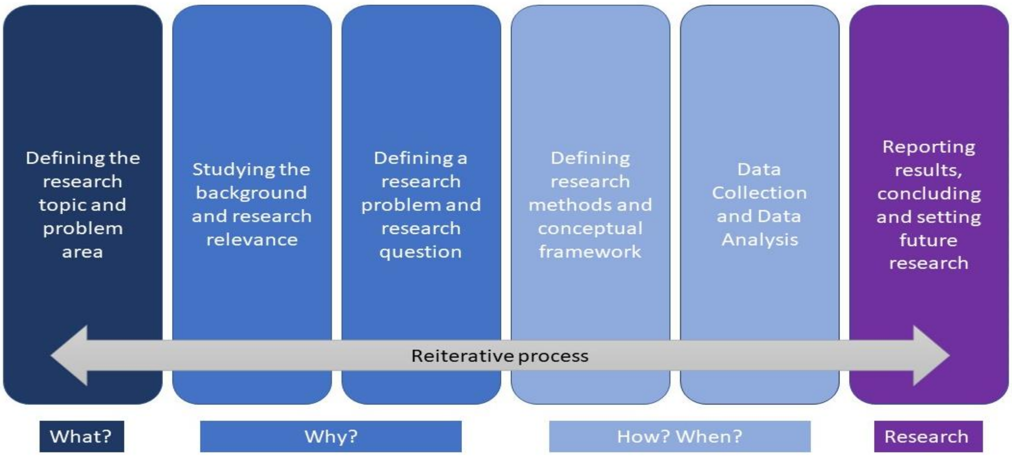
Following the definition of research subject and scope, the main reiterative process of this study was the definition of the research problem and research question. During reading, discussing, and writing a research problem and research question, the author consulted experts on the topic and received feedback from senior researchers and professors. Thus, the result is a refined research problem and research question. Figure 10 presents the reiterative steps and processes conducted to define the research problem and research questions.

Figure 10 Process of defining a research problem and research question


Defining a research problem and research question
Consulted experts, senior researchers and professors
Defining research methods, conceptual framework for data analysis and data collection
Researching the topic relevance, background and problem area

The research problem and research question defined the most appropriate research methods, data collection and data analysis. Finally, the whole process of the research and major phases conducted can be seen in Figure 11.

Figure 11 Major phases of research process


Defining the research topic and problem area
Studying the background and research relevance
Defining a research problem and research question
Defining research methods and conceptual framework
Data Collection and Data Analysis
Reporting results, concluding and setting future research
Reiterative process
What?
Why?
How? When?
Research

4.2 Research perspective and research approach

The research perspective sets the grounds for the researcher that will lead the activities of the research (Saunders et al., 2009). By defining assumptions and beliefs, researchers can create credible parts of the research design and ensure coherence between them. Scholars are stating that there are three types of philosophical paradigms: Ontology, Epistemology and Axiology. This research chooses an epistemological stance, as it concerns the researcher viewpoint of understanding what constitutes acceptable knowledge (Saunders et al., 2009). Moreover, the philosophy that leads the author and, therefore, the research is interpretivism which advocates that it is necessary for the researcher to understand the social actors and the context decisions are made (Saunders et al., 2009). The topic of this research, factors of the cross-border eID enactment, involves the factors like institutional, organisational and technological that influenced the actors' decision and enacted cross-border eID.

Because the purpose of this research is to explore the factors affecting the enactment of cross-border eID in the EU from a national perspective, partly deductive and partly inductive approaches are used. Because of the scarce literature on the cross-border eID enactment, the author needed to consult experts in the eID field to gain new insights and understandings of the research context. In addition, after gaining the understanding and new insights on eID, the author focuses and uses explained theoretical framework and literature review to construct the dimensions for the data analysis part. Because of the reiterative research process involving analysis of the scarce literature, consulting experts, the research question was redefined. This research question enabled the use of the existing theoretical framework that is relevant for the research objective.

4.3 Research strategy, choice and case selection

The choice of the research strategy largely depends on the research purpose and the research question. The research objective of this research is to explore existing factors to cross-border enactment and how to overcome those barriers from a national perspective. Furthermore, to present the commonalities and differences among Belgium and Estonia in the cross-border eID enactment and provide recommendations on overcoming existing challenges and barriers. Because there is scarce literature about the cross-border eID enactment and that the drivers and barriers are unexplored, this study will use exploratory research in order to find new insights on the cross-border eID enactment and how to overcome existing barriers hindering the process of cross-border eID enactment in the EU (Creswell & Poth, 2018).

Following the purpose mentioned above and objective, the analysis will focus on the multiple case study. The multiple case study analysis enables the author to explore the factors existing within and between cases, which is the main objective of this study. The following multiple case study follows the 'logic of replication' as Yin (2018) suggested. The logic of replication means that the findings can be replicated (Yin, 2018), which leads to the generalization of the cases (Baxter & Jack, 2008). The reason for choosing multiple cases is to find similarities and differences among cases and factors that are influencing the cross-border eID enactment.

Research choice and case selection

Regarding research choice and case selection, qualitative research is chosen as being complementary to the exploratory strategy and the research objectives. It allows using non-numeric data, which with correct applied research techniques can help to explore the existing research field and find solutions for existing problems (Bryman, 2016). Furthermore, the in-depth qualitative analysis allows new findings and understandings of the different factors that are affecting cross-border eID enactment in the EU.

The selection of the case studies follows the 'literal replication', which means that the choice of the cases should follow the logic of predicting similar results (Yin, 2018). Therefore, the starting position aims to predict similar results for the factors affecting the cross-border eID enactment in the EU.

Thus, the cases that are chosen to be explored and analysed are the countries Estonia and Belgium. The selection of these cases is based on the following criteria:

- The status of the country in the eGov benchmark for cross-border mobility, showing the development of cross-border mobility. The selected criteria are the above-average development of cross-border mobility services. For example, the DESI and e-government benchmark shows that Estonia (84%) and Belgium (60%) have the above-average development of cross-border mobility in 2019 (European Commission, 2020d).
- The participation through the eIDAS scheme and notification of eID to the European Commission. From the official catalogue of the countries that notified the European Commission, it can be seen that as of 2018, Estonia and Belgium have notified MS and the EC about their eID scheme.
- Mandatory use of eIDs and central portal access. Both countries have mandatory use of eIDs and availability for authentication through the central portal and authentication service (Pedroli, O'Neill, Fravolini, & Marcon, 2021).

- Involvement of the private sector in the provision of eID solutions. Estonia and Belgium have included the private sector as eID schemes to improve the use and access of e-services (Pedroli et al., 2021). Mainly, these solutions are for mobile authentication purposes. In the case of Belgium, “itsMe” and of Estonia “SmartID”.

4.4 Data collection

Saunders (2009) stated three ways of conducting exploratory research: a literature search, interviewing experts in the subject and conducting focus group interviews. For this research, two data collection methods are chosen: desk research and document analysis, literature review, and interviews with experts.

The desk research on the factors that affect cross-border eID enactment focus on primary and secondary data by searching for keywords such as: “electronic identity management AND EU”, “eIDMS”, “eIDAS AND cross border”, “EU AND eIDMS”, “cross-border eID”, “cross-border digital identity”, “cross-border electronic identity”. The sources used for this purpose are Google Scholar, Web of Science, SCOPUS, LIMO, and Digital Government Reference Library. Secondary data collection has been conducted in the period of the beginning of March 2021 until the end of June 2021. Because of the scope of this research, sector-specific and technology-related papers were excluded from the analysis. The literature review is conducted following the PRISMA approach, suggested by Moher, Liberati, Tetzlaff, and Altman (2009). The PRISMA approach includes four identified steps in the literature search and screening process: identification, screening, eligibility and included literature. In total, 231 results are retrieved during the search, 130 results are removed due to duplication issues, while 72 are screened for title and abstract. Full articles that are chosen as relevant and included in the research process was 38.

Following the desk research and literature review, a search for relevant stakeholders in the field is conducted. The approach towards selecting relevant interviewees is based on the non-probability snowball and purposive sampling (Saunders et al., 2009). For the Belgian case, interviewees were recommended referred by the experts and researchers in the eID field. Interviewees in the Belgian case are involved in the respective actor position, such as consultant at the local level on the eID, officer in the public sector administration related to the eID management and the stakeholder of the private organisation leading the eID scheme in Belgium. For the case of Estonia, relevant interviewees were selected based on their involvement in the eID department at the relevant Estonian Information Agency.

Furthermore, selected interviewees were referred based on their involvement in the cross-border eID. In total, fifteen stakeholders were contacted, while nine responded positively. Thus, the stakeholders involved in the eID enactment in the countries and the EU were contacted. As previously noted, in-depth interviews were chosen as the primary data collection method. These interviews enable an in-depth understanding of the experience and viewpoints of the interviewed stakeholders on the cross-border eID enactment.

Primary data collection has been conducted in the form of unstructured and semi-structured interviews from 2 June 2021 until 16 June 2021. The interview invitations are sent to sixteen relevant stakeholders, and nine responded positively. Interviewees were approached through the LinkedIn platform and by emails. Also, few interviewees are suggested and recommended by the stakeholders. Due to the COVID-19 situation, all nine interviews took place through the ZOOM platform. The interviews lasted from 28 minutes to 71 minutes. The interview protocol was developed before interviews and thus is followed during interviews (see Interview guide). In creating interview questions, the author followed the recommendation of Turner (2010), who states that interview questions should be open-ended, neutral as possible, ask only once, and be worded clearly. Following the creation of the research questions, the preparation for the interviews stage will follow the recommendations of Turner (2010) on how to prepare the stage of interviewing. Questions were asked depending on the position of the interviewee. Moreover, follow up questions were asked based on the interests and needed for more insight on the mentioned topic by the interviewee. During the interview, participants were allowed to further discuss the point of their interest under the scope of the research.

Regarding the validation of the research, validation of the research is confirmed by following the data triangulation method explained by Guion (2002). Qualitative researchers use the triangulation method to check and establish the validity of the research. Two triangulation methods are used, data triangulation which involves different sources or stakeholders in the study and expert triangulation which involved other researchers, colleagues and experts in the field in evaluating and confirming research design and interview questions.

Expert triangulation was conducted as a validation interview on 23.7.2021 with the relevant expert in the cross-border eID in the EU to discuss and validate the results and findings of this research. Furthermore, results and findings gathered through the data collection process are compared with different sources of information, thus enabling validation of the findings (Yin, 2018). Finally, Table 6 provides necessary anonymised information about interviewees and the date and length of the interviews.

4.5 Data analysis

According to Yin (2018), before the analysis process and data collection, it is important to adopt an appropriate data analysis strategy. This research follows the general strategy “Relying on theoretical propositions”, which is the most preferred strategy for the case study research (Yin, 2018). The selected theoretical framework is leading the data analysis and giving the priorities and themes for the analysis of the data. Selected propositions of the theoretical framework and research question have shaped the data collection and interview guide. Thus, the selected theoretical framework and research question helps to organise the data analysis process (Yin, 2018).

Furthermore, the research strategy should complement the research technique. In this research, the cross-case synthesis technique is selected as the most appropriate. Because this research involves multiple cases, Belgium and Estonia, the cross-case synthesis technique is most applicable, according to Yin (2018, p. 152). It is also important to note that all interviews were transcribed and analysed in the one month through several readings of the transcripts. The coding process followed the deductive theoretical framework Technology Enactment Framework by using the arrays of dimensions identified in the framework and literature review, such as technological, organisational, institutional, actors. Analysed themes are, hence, placed and categorised in the specific dimension category.

The main steps that are followed during data analysis are suggested by Braun and Clarke (2006) and Bazeley (2013). These steps are transcription, coding, analysis and writing a report. The coding process of transcribed interviews was conducted with the NVIVO 12 software programme. During the coding process, theoretical thematic analysis is chosen as the most appropriate approach following the selected data analysis strategy and data analysis technique. This is the reason because the “thematic analysis is not wed to any pre-existing theoretical framework” (Braun & Clarke, 2006, p. 9), thus enabling the best approach to use the selected Technology Enactment Framework.

4.6 Limitations of the research

Although aiming for the generalizability and reliability on the topic of cross-border eID, this research contains some limitations. There are several limitations in the research design part that are needed to be addressed. Firstly, the research question that is selected to be answered can be vague and include very broad research analysis parts due to the fact it is addressing overall factors (drivers and challenges) that affect the enactment of the cross-border eID. Thus, the research results gained are mostly general, addressing overall enactment and not specifies, *inter alia*, in the technological or organisational aspect of cross-border eID enactment.

Another limiting factor is that this research is focusing on the successful implementation of the cross-border eID. Belgium and Estonia are selected based on the successful implementation of the eID and cross-border eID, leading to the most similar design. This might lead to biased results and specific results only for developed MS, excluding unsuccessful and underdeveloped MS in terms of eID implementation and cross-border eID enactment. As addressed by the interviewee Expert F, it would be very beneficial to focus on the "current leaders and future leaders of the eID enactment".

Another limiting factor is the lack of scientific literature addressing organisational changes and implementation of the cross-border eID. Also, desk research showed that there is high debate on the cross-border eID but mainly addressing technical and legal aspects, while organisational aspects are neglected. Also, limiting factors can be found in the selected sample size of the interviewees. For example, the number of interviewees representing each actor in the enactment process of the cross-border eID could be higher. Also, each participant has been interviewed only once. Thus, it would be beneficial if participants were interviewed more than once.

A limiting factor can also be chosen cross-sectional study design, which addresses the situation at the given moment. Since the cross-border eID is still not fully functional at the EU level, this brings some limitations and perceptions of the interviewee that can be situational based. Thus, it would be very beneficial to include longitudinal studies in order to depict changes in time of the factors that positively and negatively impact the enactment of the cross-border eID in the EU.

Furthermore, this research focuses only on one primary and secondary qualitative data collection method; hence, it would be beneficial to include other data collection techniques or methods, such as quantitative methods and surveys.

5 Case study countries

5.1 Belgium

5.1.1 General Information and digital development

Belgium was a founding member of the European Economic Community in 1958, and it is a high-income country with a current population of 11.5 million people (Eurostat, 2019). Belgium is geographically situated in the west of Europe, bordered on the north by the Netherlands, east by Germany and Luxembourg and south by France. By gaining independence in 1830, the country experienced several reforms in the pollical system. Between 1970 – 2001 the country reformed into the federal political structure, reformed into Belgium that is known today (Leyman, 2012). The federation of Belgium is composed of communities and regions (Leyman, 2012). The main distribution of power is based on the two lines, the language or the culture (communities) and on the economic interest (regions) (Leyman, 2012). There are three communities in Belgium the Dutch Community, the French community, and the German community. The state reform towards federation also created regions based on economic interests (Leyman, 2012). As a result, there are three regions in Belgium, the Flemish Region, the Walloon region and the Brussels capital region. Hence, Belgium is a federal constitutional monarchy, where power is divided among Federal Government, Regional government and three communities (Dutch, French and German).

Being ranked as one of the top-performing countries among the EU MS, Belgium has one of the highest connectivity rates to the Internet (European Commission, 2020d). Hence, the citizens of Belgium has a higher rate of internet usage than the EU on average, 59 % and 53 % (European Commission, 2020d). Also, the Belgian citizens have access to the most automated services, with 23% fully automated services(European Commission, 2020d). This means that citizens are not required to request services, but they are proactively provided. However, although Belgium has provided great internet connectivity and access to online services, it has a lower usage of the services by the citizens. This means that citizens are not actively using their provided services; hence, Belgium is positioned under the expandable government in categories. The category of expandable government addresses the issue of low awareness of citizens and low penetration of the accessible services in the country. To address these issues, Belgium has adopted strategies and policies related to the development of the digital government.

The Federal government of Belgium adopted in 2009 the “Federal eGovernment strategy”, and it is still in force. This strategy's main objective is to create a single virtual space for public administrations and access to online services by the citizens and businesses (European Commission, 2020b). The strategy goals are to enable optimal service delivery to citizens, to reduce administrative burden and to enable higher efficiency and effectiveness of public services. Furthermore, it provides a common vision for using the information management systems and information security, such as standardisation in information modelling. Another outlined goal was to maximise the use of the common elements, among other things, eID building block. To achieve the above-mentioned objectives, the strategy is based on the four main strategic streams. The first stream is focused on the user needs and simplification of the administrative procedures. The second stream is focused on the cooperation among government entities and administrations to provide integrated and interoperable services across organisational boundaries (European Commission, 2020b). The third stream focuses on simplifying administrative procedures by enabling data and information exchanges among public administration (European Commission, 2020b). Finally, the fourth stream affects the back-office integration and data privacy protection by enabling a department or agency responsible for the authoritative sources. In addition to the Federal eGovernment strategy, in 2015, Belgium has adopted a Digital Belgium action plan. Digital Belgium action plan has the objective to promote growth and create jobs through digital innovation (Federal Government Belgium, n.d.). To achieve these objectives, this action plan has set specific policy goals in five main pillars. These priority areas and main pillars are digital economy; digital infrastructure, digital skills and jobs, digital trust and digital security, and digital government. One of the initiatives to be launched within this action plan is, inter alia, a mobile authentication for eGovernment applications.

According to Mr Frank Leyman, manager of international relations at the Federal department for ICT in Belgium (BOSA), eID is the essential building block of the Belgian e-government strategy (Leyman, 2012). Currently, in Belgium, there are two eID means to identify and authenticate for online services, the Belgian eID (BeID) public identity provider and itsMe private authentication provider. The analysis of the eID schemes is based on the notification of the eID schemes by Belgium, according to the eIDAS

Regulation. Belgium notified eID schemes in 2018, and those are the National Belgian electronic identity card (BeID) and itsMe eID scheme.

5.1.2 Enactment of eID in Belgium

Following the EU Directive 99/93 on the electronic signatures, Belgium decided in early 2000 to plan the development of electronic identification and digital version of the paper-based ID (De Cock, Wolf, & Preneel, 2006). The first pilot phase of provision and use of eID was in 2003 by issuing the eID cards to the civil servants (De Cock et al., 2006). The production and distribution of the eID cards to the municipalities has been awarded to the private company NV Zeves, which was already involved in the provision and production of the social security cards (Mariën & van Audenhove, 2010). In addition, the production of authentication certificates is awarded to CERTIPOST. The national roll-out started in 2004, and municipalities are in the process of issuing eID cards to citizens. Only Belgian citizens were able to receive this eID, until 2008 when the foreign nationals residing in Belgium were entitled to replace their old paper ID with the eID. Furthermore, Belgium provided eID cards to children older than 12 years as of 2009. The main difference is that eID for kids contains the contact phone of the parents or guardians and does not have a signature certificate.

Having a personal identity document is mandatory in Belgium, and all citizens and legal residents are required to receive a Belgian eID card. Every eID mean in Belgium contain a national registry number that is provided to every Belgian citizen and resident. National Registry Number contains 11 numbers, and it is created by: first six digits are citizen's date of birth; followed by three digits which is serial number; with final two digits which are checksum digits.

The second notified eID scheme is the itsMe, Belgian Mobile-ID. Belgian Mobile ID is a company that is behind itsMe authentication application for mobile authentication. It is mainly founded for the purposes of authentication for the private world, according to Expert G. The founders of the Belgian Mobile ID are four main bank companies in Belgium KBC, IMG, BNP and Belfius, together with the three telecom operators (Expert G). Since 2017 and the adoption of the Belgian law on electronic identification, itsMe submitted an application to become the first mobile authentication service for the public services. Since 2018 itsMe is the first private company providing mobile eID to the citizens in Belgium.

So far, there are 2.7 million registered users that created an account in Belgium (24.5% of the whole population. The total transactions conducted with itsMe app accounted for nearly 10 million.

Technology

BeID card is a regular smart card that contains an electronic chip. On the physical smart card, BeID contains the necessary information, inter alia, Name, Surname, Date and Birth, gender, signature, citizenship, national registry number, while excluding the address of the eID card holder[7] (Thales Group, n.d.). Moreover, BeID contains two certificates on the chip; one is for authentication on the portal, while the other is for the digital signature. When electronically read, the BeID card provides three files. One is the picture of the eID holder, and the second one is the so-called "identity file" that contains identity information with a unique personal identifier and an image of the person. The third one is the address file, which contains the information of the current address of the eID card holder. The identity and address files are digitally signed and tampered by the National Register in Belgium, which affirms the validity and authenticity of the files (Fairchild & de Vuyst Bruno, 2012). The latest eID contains biometric information next to the picture, fingerprints of the BeID holder (Thales Group, n.d.). The technology that is chosen to be implemented in the BeID are decided in the beginning of the development with few updates. It is decided for the smart card with a chip that contains as already mentioned two certificates and three files. Regarding the encryption and Public Key Infrastructure information, it uses the two X.509 certificates which are stored on every BeID card (Roelofs, 2019). The communication protocol is PKCS#11, which are complied with the ISO 7816 standards for smart cards (Roelofs, 2019). Having software and additional means such as smartcard readers and then entering 4-digit PIN code, BeID fits under the LoA high, according to the peer-reviewed process.

For ItsMe, the solution is based on the smartphone application. The specificities and characteristics of the itsMe application cannot be accessed because it is a closed-source application. The authentication mechanism is based on the PIN code, which can later be changed with biometric recognition. The authentication flow is connected to the FAS needed for authentication for public services is based on the OIDC and TLS standards (Belgium, 2018).

Organisation and actors involved

The organisational governance and actors involved in provision and distribution of the BeID, range from the public sector of governance role to private actors of manufacturing and certification issuance. Main stakeholders responsible for the BeID and digital identity are Federal Public Service Policy & Support / Directorate General Digital Transformation

[7] Address information is excluded because of the possibly often changes of the address information.

(BOSA / DG DT), The National Register of natural persons, Municipalities, Federal Public Services for Home Affairs and appointed private companies.

Municipalities are responsible for issuing the cards to the citizens and responsible for issuing the requests for manufacturing procedures of the eID cards. The manufacturing procedure is the responsibility of the private company appointed by the Council of Ministers (Belgium, 2018). The auditing organisation that perceives the process of manufacturing and issuing is the Federal Public Service for Home Affairs, also responsible for the two files.

National Register is responsible for managing the authoritative sources' databases that contain all the unique personal identification numbers of the citizens. This Unique personal identification number contains 11 numbers allocated in an automatic manner (Belgium, 2018).

The BOSA is a federal unit in Belgium founded in 2001 that acts as the leading actor in developing the eGovernment strategy. More specifically, it also develops cross-border frameworks and data exchange federal systems (Leyman, 2012). Hence, the BOSA is responsible for the authentication procedure and maintaining Federal Authentication Service (FAS) that enables cross-border authentication. Furthermore, the BOSA is responsible for the cross-border authentication process and implementation of the eIDAS nodes and cross-border eID.

In the itsMe notification documents provided to the EC and MS, the organizational governance and actors that are involved in the itsMe eID. The two entities are responsible for enabling a private eID scheme in Belgium. First is, as already mentioned, Belgium Mobile ID (BMID) company is a joint venture of banks and telecom companies. BMID is responsible for the issuance and all operations related to the itsMe authentication and services and mobile itsMe application. This company is also responsible for the correct collection of identification data for its users from the Identity Registry that contains data from Belgian citizen eID cards. Also, the company is responsible for the operation of authentication procedures. Thus, BMID forwards the national identity number to FAS, which creates the minimum data set of that personal identification data based on that authentication (Belgium, 2019). Second is the BOSA that regulates and operates FAS, which provides a central gateway for authentication. The FAS handled more than 55 million authentication in 2018 (Belgium, 2019).

Legal framework

In Belgium, the mandatory use of identity documents has been provisioned since 1983 (Mahula, 2020). Since then, with the advancement of the ICT and internet, Belgium adopted several legal documents that regulated and enabled electronic signature and identity. First one was the Royal decree on the legal framework of electronic ID cards from 2003 (2003-03-25/31) (European Commission, 2020b). This is one of the first institutional initiation and frameworks of the provision eID cards in Europe. Then, in 2004, Federal Government adopted the Royal Decree 2004-09-01/33 on the generalisation of the eID cards (European Commission, 2020b), which legally enabled the use of the eID cards and its signatures, with the adoption of the Royal Decree on the Belgian kids' eID card.

The latest legal development was adopting the Belgian law on electronic identification, adopted in 2017, Royal decree of 22 October 2017. This law is complementary to the eIDAS regulation. In this regulation, Belgium, for the first time, recognized a private solution for authentication itsMe. As a result, all citizens are able to authenticate from mobile phones, which FAS offered.

5.2 Estonia

5.2.1 General information and digital development in Estonia

Belgium is the ex-Soviet Union country that gained independence in 1991. Since then, Estonia started developing a democratic country focusing on IT and digitalizing the public services and developing its eGovernance model (Anthes, 2015; Nielsen, 2017). In 2004, Estonia officially joined the EU. A small Baltic country with 1.32 million people borders Finland on the north, Russia on the east, Sweden on the west and Latvia on the south. After the fall of communism and gained independence from the Soviet Union, Estonia has built a unitary state with a highly centralized political system (Nielsen, 2017). In Estonia, there are 183 rural municipalities and 30 city municipalities with minimal financial and human resources, hence resulting in minimal service delivery capacities, according to Nielsen (2017, p. 4).

In Estonia, one of the pioneering countries in the utilization of IT in government, around 85% of the population uses the internet, according to the Eurostat (European Commission, 2020c), conversely to the EU average of 55%. Furthermore, Estonian citizens interact with the government by filing and receiving documents online with 60% of individuals and 75%, respectively. One of the main economic sectors in Estonia is the ICT sector, with 5.9 % employees and more than a thousand start-ups (e-Estonia, n.d.).

According to the EU e-government benchmark, Estonia is a leading country in the EU in e-government (European Commission, 2020d). Also, in the category of the key enablers that include eID, eDocuments, Authentic sources and Digital Post, Estonia has the second-highest results achieved with 93%. Furthermore, in contrast, this is also relevant for cross-border mobility, which shows the possibility for cross-border use of the e-services, which are in the case of Estonia, about 85%.

This success in digital government had been supported with several political and legal decisions, strategies and acts. Since independence, the use of ICT has actively been pursued in Estonia (Nielsen, 2017). Estonia's first important strategic documents the 1998 document on the "Principles of the Estonian Information Policy" (Nielsen, 2017). With this document, Estonia committed to, inter alia, focus on the development and roll-out of the government ICT infrastructure, on developing the eCommerce and eBanking and improve defence by utilizing ICTs (Nielsen, 2017). This strategic document was in force until 2004, which was upgraded with the new "Estonian Information Society" action plan that included, inter alia, promotion and introduction of e-services to citizens, businesses and governments, roll out of eID cards, increase public sector productivity through ICT and data exchange infrastructure. After that action plan, Estonia developed the "Estonian Information Society Strategy" in 2007 that was planned for the next six years until 2013. The main objectives, inter alia, of that strategy, which was aligned with the EU action plan, was to improve multichannel service delivery, to improve digital literacy of up to 70% of Estonians, and that 15% of GDP is generated by the ICT sector. In 2014, Estonia developed the latest "2014-2020 Digital Agenda: Estonian Information Society Strategy", which focuses mostly, inter alia, on the smart solutions and enabling infrastructure, use of eID and eSignature services, increase cross-border cooperation on data exchange, eID and eSignature, and to promote eResidency programme (Nielsen, 2017).

According to Nielsen (2017), historically, Estonia has spent a minimum of 1% of its annual budget on ICT and information society activities. Interestingly, 85% of government spending on egovernment has been funded by the EU structural funds and programmes.

5.2.2 Enactment of eID in Estonia

After complete independence from the Soviet Union, Estonia had still used traditionally paper-based ID documents (Martens, 2010). Since 1997, Estonia has discussed and planned the issuance of new identity documents, led by the Estonian Ministry of Interior (Martens, 2010). The discussion about the new identity document involved stakeholders from the public but also the private sector. Thus, the result of the discussion was the agreement upon the path to produce and provide eID cards to all citizens of Estonia. The first Digital Signature Act was adopted in 2000, three years after the initial agreement on the eID cards in Estonia (Martens, 2010). This adoption of the Digital Signature Act was in line with the EU Directive 99/93 on the digital signature, assuring the primary set objective of the Estonian government for membership in the EU. Since the Digital Signature Act, two companies were founded to be involved in the new eID project in Estonia (Martens, 2010). The eID companies were founded by the leading banks and telecom operators in Estonia. Thus, confirming the importance of the Bank and Telecom sector in the eID field, mainly for digital signature purposes. These two companies were responsible for card manufacturing procedures and the issuance of the certificates. One of the crucial moments, according to Martens, for the success of the eID projects in Estonia is the decision that all eID cards should be equipped with chip and certificates and that eID cards should be mandatory for all citizens of Estonia (Martens, 2010). This decision was made by the falling government in 2001, and it confirmed that the project of implementation of the eID had not been affected by the changes in the political sphere (Martens, 2010).

The First Estonian eID card was issued in 2002, and the first period of distribution of eID cards showed the low take-up due to the lack of awareness, lack of applications and concerns about investments in the eID cards (Martens). Currently, all citizens of Estonia has at least one of the eID means which might be used for identification and authentication for online services. eID means that are provided to Estonian citizens are ID-card, Mobile-ID, e-Residency and Smart-ID.

Since 2017, Estonia provides also a digital identity for citizens of other countries than Estonia. This is possible for everyone who plan to start a business in Estonia. The project that provides digital identity is called e-Residency[8]. Through this project, a citizen of any country in the world can gain access to all e-services as Estonian citizens and residents. The goal of e-Residency is to enable access to digital services of Estonia to anyone who would like to become an e-resident due to the fact that access to services should not be

[8] For further information about e-Residency project, please see: https://e-resident.gov.ee/become-an-e-resident/

dependent on the physical location of the entrepreneur or business (Aavik & Krimmer, 2016).

Every Estonian citizen and resident, or e-resident, contain a personal identification code as a unique personal identifier on the eID means. Estonian personal identification code consists of eleven digits and is regulated by the act on " Procedure for creating and issuing personal identification codes". The formation of the personal identification code is following:

Table 1 Estonian personal identification code formation (Procedure for formation and issuance of personal identification codes - Riigi Teataja, 2021)

1) the first number	1 - a man born between 1800 and 1899;
	2 - a woman born between 1800 and 1899;
	3 - a man born between 1900 and 1999;
	4 - a woman born between 1900 and 1999;
	5 - a man born between 2000 and 2099;
	6 - a woman born between 2000 and 2099;
2) the second and third digits	- the last two digits of the year of birth;
3) the fourth and fifth digits	- month of birth number (January - 01, etc.);
4) the sixth and seventh digits	- date of birth (01, etc.);
5) the eighth, ninth and tenth digits	- serial number for those born on the same day;
6) the eleventh number	- control number. The control number is presumed to be compliant if it is calculated according to the rule in the standard.

For cross-border services and mutual recognition, Estonia has notified four eID schemes for mutual recognition in the EU. Notified schemes are Digi-ID, ID card, Mobile-ID, Residence permit card and diplomatic identity card. Thus, because of the scope of this research in the following sections, only the notified eID schemes are discussed.

Technology

Technologically, Estonian eID cards are based on the smart card and card reader for authentication. The only notified solution that is not containing a smart card is Mobile-ID. The Estonian eID schemes are based on the Public Key Infrastructure (PKI) by utilizing SSCD/QSCD smartcards (Police and Border Guard Board Estonia, 2019). These private keys are kept on the chip of the eID smart cards, while on the Mobile ID, it is kept on the SIM card (Police and Border Guard Board Estonia, 2019). All Estonian eID are compliant with the latest international standards and fulfil the ISO/IEC 7816 standards for eID and e-signatures (Police and Border Guard Board Estonia, 2019).

Two certificates that are kept on the Estonian eID card chip contain two private keys that are saved on the X.509 format (Police and Border Guard Board Estonia, 2019; Roelofs, 2019). One certificate is used for electronic authentication and encryption, and the other is used for electronic signatures. These certificates are valid until the end of the validity of the eID card (Roelofs, 2019).

Organisation and actors involved

As already mentioned, Estonia provides six eID schemes. Three of them are physical identification documents (ID card, diplomatic identity card and residence permit card), and the other three are digital identity cards (Digi ID, Mobile ID and e-Residency).

The organisation of the eID schemes in Estonia is considered a good example of the relationship between two types of parties, public authorities and private parties, in the governance of the eID schemes (Martens, 2010). The involvement of the private parties at the start of the development of eID is considered as one of the important factors of the success of eID. Furthermore, the success of the high uptake of the eID cards in Estonia, scholars accredit to the organisation of the identity management, existence and use of the centralized unique personal identifiers for all residents, and centralized data exchange infrastructure in Estonia, X-Road (Martens, 2010).

Public authorities are mainly responsible for the issuance and supervision of identity management systems. In Estonian eIDMS, the Ministry of Interior is the leading actor and is responsible for policies in identity management and the issuance of identity documents. The directory of the Ministry of Interior, the Estonian Police and Border Guard Board (PBGB), is responsible for issuing the identity documents to the Estonian Citizens, thus called “the issuing authority” (Police and Border Guard Board Estonia, 2019). Also, the PBGB performs as a single point of contact for cross-border needs, according to the eIDAS regulation (Police and Border Guard Board Estonia, 2019).

Another important public institution that is involved in identity management in Estonia is Information System Authority (RIA). RIA is considered as a supervisory body that is responsible for all requirements set up in the eIDAS regulation. Responsibilities of RIA in the field of eID include, *inter alia,* developing the vision and strategy for the field of eID, for interoperability of international electronic identities, and responsible for the functioning, development and management of ID-software’s for end-users.

On the other hand, private parties are contracted by the public authorities for the tasks that are not carried by the public authorities, such as manufacturing processes and market roles (Police and Border Guard Board Estonia, 2019). For the manufacturing and personalization of eID cards in Estonia, PBGB contracted private company Gemalto AG for 3rd generation eID cards and IDEMIA for 4th generation of eID cards. Furthermore, next to these companies responsible for manufacturing and personalisation of the ID cards, PBGB contracted certified certification service provider, SK ID Solutions is responsible for issuing the certificates for national identity cards in Estonia, thus responsible for all processes from verification to suspension or revocation of certificates (Police and Border Guard Board Estonia, 2019). The founders of SK ID solutions are banks and telecom operators in Estonia, SwedBANK, SEB Bank and Telia Eesti (SK solutions, n.d.). For the Mobile-ID, companies that are contracted are Telia Eesti AS, Elisa Eesti AS, Tele2 Eesti AS. They are responsible for the issuance of the SIM cards that have functionality for electronic signature and electronic authentication (Police and Border Guard Board Estonia, 2019).

Legal framework

In Estonia identity documents are regulated by two acts, Identity Document Act and Electronic Identification and Trust Services for Electronic Transactions Act (RIA.ee, n.d.).

Identity Document Act was adopted and passed in 15.2.1999. This regulation establishes requirements for identity documents and also regulates the process of issuing identity documents to Estonian citizens and residents (Identity Documents Act, n.d.). This legal act has been amended several times since its adoption in 1999. The last amendments in the Identity Document Act entered in force on 01.02.2020. With this document, all eID means that are issued by the Estonian government are regulated.

Second act that is regulation the eID field in Estonia is the Electronic Identification and Trust Services for Electronic Transactions Act. The first adoption and entry in force were from 26.10.2016. This act is the primary act that regulates eID and e-signatures in Estonia, which is national law applying eIDAS regulation. Within this act, supervision and competence authorities for eID in cross-border settings are defined.

5.3 Summary and comparison of case-study countries

In Table 2 short summary of described case study approaches on eID enactment from national perspective is provided.

Table 2 Summary of case-study countries

		Belgium	Estonia
General Information	**Political System:**	*Federal system*	*Unitary system*
	Population:	*11.5 million*	*1.32 million*
	Digital Development:	*Top performing country*	*Top performing country*
Enacted eID	**First issued eID:**	*2004*	*2002*
	UPI:	*National Register Number*	*Personal identification code*
	Notified eID scheme:	*BeID, itsME*	*ID card, e-Residency, MobileID, RP card, DigiID*
	Use:	*Mandatory*	*Mandatory*
Organisational dimension	**Leading actor:**	*BOSA*	*Ministry of Interior – PBGB, RIA*
	Certification and manufacturing actors:	*CERTIPOST, NV Zeves*	*SK ID Solutions, Idemia*
	Issuing authority:	*Municipalities*	*PBGB*
Legal dimension	**Legal documents:**	*Royal Decrees on eID*	*Identity Information Act, eID and Trust Services for Electronic Transactions Act*
Technological dimension	**Credential technologies:**	*Smartcard, Mobile App*	*Smartcard, Mobile App*
	Certificates	*X.509*	*X.509*
	Communication protocol:	*PKCS#11*	*PKCS#11*

6 Results

The results of the data collection from the interviews and supportive literature for Belgium and Estonia is presented in this chapter. The structure of this chapter is based on the Technology Enactment Framework, which is used as a theoretical framework for data analysis of the interviews. Thus, the main dimensions of the mentioned framework were used to categorise themes that resulted from the analysis of the interview transcripts. The forementioned dimensions are technological factors, organisational factors, institutional factors. In addition, as one of the objectives of this research is to present the standpoints of Belgium and Estonia towards the new proposed European Digital Identity wallet, their perspectives are also presented in this chapter.

6.1 Belgium

6.1.1 Technological factors

Existence of the unique and persistent personal identifier

In Belgium, since the early 1960s and 1970s, started to uniquely identify its citizens through civil administration (Expert E). Then in the 1990s, Belgium has created a centralized database, so-called National Registry database. Thus, with the development of the new ID card in 2002, which contains electronical function and it is "*a materialisation of your registration in the centre of register. So the basic thing is, you have a central register*" (Expert E). Expert F also says "*so they did a good job for the central registry that involves everybody.".*

According to Expert G, the existence of the national unique identifiers helps even digitalization of the country. Expert G stated, " *that (national registry number) also helps in the digitization of a country".* Furthermore, this existence of the unique and persistent personal identifiers "*helps of course to create a digital identity*" (Expert G).

Also, the inexistence of unique and persistent identifiers in other MS is perceived as a challenge for cross-border eID. According to Expert G, "*for example, if you look at France, it will be very difficult to have a digital identity the day after tomorrow in France, because they don't have electronic identifiers, they don't have a national registration number*". Moreover, Expert F in other way considers the existence of unique personal identifier in Belgium can have some drawbacks. According to Expert F, "*what is also a bit of problematic in a sense, if you compare that with Germany, in Belgium, we all link it to that national registry number. There is also a problem in correlation. Of course, I, you see that in Belgium, if you go to Mediamarkt, one of those big centres, they ask you I* *can I put your warranty on your ID? Yeah. They save your national registry number. Yeah, so potentially get a lot of correlation between a lot of things*.”.

Federal Authentication Service

Another technological factor that is perceived as an important driver for the enactment of the cross-border and national eID is the existence of the Federal Authentication Service (FAS) in Belgium. According to Expert E, in Belgium, they are very satisfied with centralizing authentication service, “*First thing we are in Belgium very happy that we have only one federal or let's say governmental authentication system. It's called the Federal Authentication Service. Meaning that everybody who wants to access online applications or federal government has to go through that front door*.”.

Furthermore, for private actors who operate the eID scheme in Belgium, FAS is also important aspect of success, compared to other countries like Netherlands, according to Expert G. According to this expert, involvement in other countries identity provider can be difficulty towards their authentication system. For example, “*I think they're in the Netherlands, we're doing it too, because actually, the way it's work, it's a little bit different than Belgium. In Belgium, we have one federal hub that is used by by cities and the and the government in the Netherlands is different, because you have the federal level, and then you have on cities*.” (Expert G). Mainly, FAS enabled more often use of the private provider eID scheme by citizens. For example, Expert G mentioned “*so actually, we had one implementation, and then we have like, I think 1000 applications behind FAS to log in, so it's for your taxes or for a lot of different things. So it is all the public sector.”.*

Legacy system

A legacy system is also considered an important factor that has a positive but also a negative impact on the cross-border eID. According to Expert F, *“Belgium has an advantage and disadvantage in their early adoption of eID.”.* Advantages of their early development of eID and its legacy systems are sense which enables easy implementation of cross-border eID.

However, as stated by Expert F, “*there is a challenge with a legacy”* mostly based on the experience of the already existing system that is not adapting towards the new trends and use of mobile phones.

Moreover, Expert H addresses issues on the EU level caused by legacy systems in Member State by stating, “*as you know, now, each member state they create their own national systems. They don't have any common standards, no commonalities at all, sometimes, and it can be quite tricky to make them function cross border*.”.

Thus, mobile phones and identification and authentication through mobile phones are considered as the primary goal and pathway for cross-border eID by the interviewed experts from Belgium.

Data interoperability

In cross-border e-services, it is of crucial importance to enable seamless data interoperability between countries and technological systems. Within the eID, identity is not just a given number that uniquely identifies a person but also other attributes and credentials that are not included in the eID cards. Expert F confirms this claim by saying, "*It's a lot of other credentials that are also part of the identity. And that is not included in the eID*". Furthermore, Expert F says, "*it's not only about identification, but your basic credentials. It's about also adding new data".* Expert G also states that "*identity is more than only a registration number and a given and a name, and a date of birth.".*

Thus, this data that is part of the identity has to be shared across borders and is important for achieving cross-border eID. It is considered that data interoperability "*is a huge challenge*" according to Expert G. Furthermore, Expert G emphasises the importance of cross-border data exchange situations, "*because we, I like to travel as much as you are doing. And so when you change country, it's very difficult to have the information that you have in one country to take it to the other country. It could be medical, it could be financial, and so on. So I think as we are all moving in the EU, we need to have some tools like that.".*

High security level of assurance

Another important technological factor that was mention that affects the enactment of the cross-border eID is the requests for high-security eID while usability is mostly neglected.

The effect that highly secure solutions that governments primarily follow can have on the market of eID can be that citizens are turning towards private corporation identity providers such as Apple or Facebook, according to Expert F. Furthermore, Expert F addresses the high level of assurance in eIDAS by saying, "*So if they put only on high secure, high level of assurance aspect, then you have a problem. Most people will say okay, it's highly secure. But I prefer a Facebook called Apple ID, which is easy to use, right? So easy to use, okay, they steal my information, but at least it's easy*."

The main reason of highly secured solutions request multiple card readers to verify identity, which has driven creation and use of itsMe eID scheme in Belgium. Expert G mentioned, "*Because in Belgium, we love card readers. So we have we always used in the past, or bank card in a card reader. But for foreigners, they always look at it, like how many card readers do you have? So you can use it's me to replace your card reader*.".

However, as mentioned by Expert F, "*you need to balance those things (security and usability).*"

6.1.2 Organisational factors

Approaches towards cross-border eID

In the EU, there are different approaches towards the solution of enabling cross-border e-governance. Mainly, organisations are concerned about sharing data across borders caused by a lack of trust and knowledge of procedures (Kalvet et al., 2018).

In Belgium approach towards its unique personal identifiers of its citizens and businesses is that they don't share it outside of public sector (Expert J). Thus they are reluctant towards sharing unique personal identifiers across borders. Expert J mentioned, " S*ince in Belgium, you know, we have our national register number, which is kind of the pillar of the identification system that we use. But traditionally, we have the rule that only governments are allowed to use it. So that makes it a lot harder*".

To enable identity matching in Belgium, it is provided with an eIDAS ID through an eIDAS node that is correlated with a Belgian national register number if an entity has one. The use case of this approach is explained by Expert E, *"I come in with my Italian identity into eIDAS in the Belgium note. At the moment I've come in, I receive in Belgium the eIDAS node receives given name, surname date of birth. Then we are looking into our database, can we find somebody with Name and Surname, date of birth? Yes, we find a match. If the match is 100% we know immediately his national registry number. And we correlate his Belgian national number with his eIDAS number. But you can get as much as numbers as you have identities in other countries. And any one country can get more than one identity."*

Trust mechanism

Trust is an essential element for the identification and verification of persons. Trust in identity documents are usually based on authoritative government sources that provide pieces of evidence and credentials about a person's identity. Expert E, mentions "*You don't know, the only thing is that governments and Belgium people accept Belgian ID. Because they trust it, they can verify it against an original source, which is a guarantee that all these elements are correct. They guarantee it.".*

In cross-border settings, there is a need for the creation of agreements between MS in order to accept identities from each other. The framework for trust is needed, according to Expert F, *"you need to establish a trust framework that every party agrees on."*.

Furthermore, Expert E states that identity should be sovereign and cooperation and agreements between countries outside the EU will often peer to peer agreements, *"sovereign means you have to establish agreements or regulations. MS, between countries, outside Europe, it will be peer to peer agreements".*

Development of ID for national purposes

Interviewees mentioned a factor that is affecting the current enactment of cross-border eID, a factor of the design and focus of eIDs for national services and its citizens.

"I think a fundamental problem. It is a national ID, I am that person in Belgium, and in France, I am another person.", mentioned Expert F.

The creation of the eIDs was just focusing on the electronic functions of the provided cards, neglecting the purpose of cross-border e-services back in time. Thus, Expert F states that "*I think the problem there was always that it was always consigned conceptualised as national ID working for that context, the world has evolved.".* Nowadays, "*we see a lot of more interactions and persons have multiple IDs"*, which comes as a driver for evolutional eID.

Also, the provision of identities are heterogenous; every Member State provides its own identity with its own procedures and rules. As noticed by Expert E, "*I can own more than one identity I can own an identity in Italy and identity in France and Belgium and I can have the content of that identity is not always the same.*".

Also, it is noticeable by Expert H that there the cross-border eID has not been "*has not been on the top of the agenda in MS because they have not really seen the usefulness, I think of fully implementing the technical interoperability between the nodes.*".

6.1.3 Institutional factors

Limited eIDAS framework and success

Legally the eID in Belgium focuses mostly on public sector and it was unable to be used for private services, thus affecting lack of use of eIDs. As noted by the Expert F, "*with all due respect, you have interaction with public sector, but is not your daily interaction, or you pay your taxes you log in and in taxation are the ones maybe you once login fundament as well, too, but that is it".*

Furthermore, regarding eIDAS regulation on the institutional part and its implementation to enable cross-border mutual recognition of eID, Expert F mentions that "*the other problem that maybe on the general ways, of course, it was all, only uptaken by the public* *sector"*. Expert I also claims that with eIDs, there is a lack of usefulness in terms of services that are provided by the public sector because it only focuses on public sector services. Expert I stated, "*And another factor is the private sector involvement. with digital identity, governments tend to focus on public sector use cases, like tax declaration, example, but you do that once a year."*

Another important aspect of the legal part of eIDAS was with the notification process of eID schemes in the EU. With the eIDAS notification process, eID schemes are notified by the MS and being accepted only in Member State. Expert G, claims that it should also be involved the use of eID schemes in other MS states as well by saying, "*I would say that once you recognise in one country that you can add, actually other countries. Because that is not the case, we have to do the whole audit again, to be first recognised by the Netherlands and then on European level.".*

Thus, an update on eIDAS regulation is expected and necessary, "*because today, it's a national regulation, so you cannot create cross border solutions."*, according to Expert G.

Also, as addressed by Expert G, planning of business involvement in the cross-border setting is neglected. Expert G stated, "*We have, for example, in Belgium, it's the royal decree that says how much we are paid, we need to have a private activity next week. So we're either opening up to Europe, and there is no remuneration part link to it.".* Furthermore, it is necessary to have a plan how to involve private eID providers into the cross-border schemes, according to Expert G.

Mobile government trends

In Belgium, interviewees mentioned mobile government as an important aspect of the future regarding eIDs. With the development of mobile phones and more often use of mobile phones, in Belgium, they were using eID smart cards and card readers for computer identification and authentication.

Expert F stated *"It (eID) worked indeed, card reader and with desktop application. And when the new mobile aspect came around, they had a problem".* The reason of usability and more often use of mobile phones, came to the acceptance of itsMe in the public sector, according to Expert F and Expert G.

Expert E pointed out that public administrations and governments nowadays are focusing more on the mobile app development and mobile government. Expert E stated "*more and more administrators are no longer developing online application. But they are developing apps on Android, apps on iPhone apps. on Chromebooks apps on Windows, because with* *an app, you have much more possibilities to control to drive to manage your user user experience, and to protect it.".*

Moreover, Expert H noticed that eIDAS regulation lack success and noticed that eIDAS did not have a legal obligation for MS to notify eID scheme. This is explained by saying, "*the first barrier is, of course, the legal one, or the lack of obligation on MS to notify their IDs. So that, of course, is a big barrier."*

Political effect, digital transformation, COVID-19

Political support is also perceived as an important factor by the Expert G and H. With the political parties and their position on left and right scale, and it can be slightly acknowledged whether it will focus more on centralized or decentralized development of the eIDs, according to Expert G.

Furthermore, Expert I claims that currently there the problem is not funding by saying "*So I can tell you one thing that I was surprised that isn't a block and that's money. And it's really not why things are not working. There's so much funding for digitization right now".*

Also, cross-border is not a main purpose of the politicians but rather national development of e-services and national needs, according to Expert I. Expert I explains *"the average European citizen, I think the main benefit is going to be at a national level".* Also, due to that institutional legacy, to allow eIDs to work across-border, there should be significant changes in the laws and in organisations, according to Expert I.

Next to the political effect, interviewees mentioned also institutional focus on digital transformation. Mainly, after COVID-19 it was reassured that digital transformation of government was necessary. Expert E states, "*Okay, digital transformation is driving is driving the change. Especially Corona is a catalyst for it. Oh, no, no, it pushed us forward 200 miles an hour".* Expert F also agrees on this point, mainly that with the COVID-19 also affected in great matter the cross-border procedures. Also, e-services are just not ending on the identification of an entity but also requires additional steps to become automated, according to Expert F. Expert H is also agreeing on this point by saying, "*the main driver in this whole process has been the COVID. Because that one has really accelerated the demand for trusted and secure e IDs."*

6.1.4 Opinions on the Proposal and European Digital Identity Wallet

Three experts from Belgium gave their insights on the perspective on the new eIDAS proposal of the amendments on eIDAS regulation and within it creation of the European

Digital Identity Wallet. The reason is that an interview with Expert G was conducted before publishing a new eIDAS proposal.

Mainly, the opinions of the interviewees regarding the implementation of the new eIDAS proposal was quite positive, with few concerns related to the development and governance of the European Identity Wallet. Interviewees believe that the new SSI approach will solve existing issues with data interoperability and lack of credentials, mostly due to the fact it is based on the user-centric model of the eIDMS. According to Expert F, with new eIDAS proposal and with the new European Identity Wallet, "*It's not only about identification, but your basic credentials. It's about also adding new data. So attributes that you can use that show the extent is bigger. And they also put the user in the centre of it.".*

Challenges in another hand, are related mostly to the governance of the cross-border European Digital Identity Wallets. Due to the fact that every Member State has a sovereign right to independently develop digital identity wallet, it is perceived that then all MS collaborate and develop interoperable wallets, according to Expert F. Furthermore, similarly to the first eIDAS regulation, there is a lack of inclusion of other stakeholders in the eID. Expert F mentions "*They don't have really a vision or clear understanding how to include the private sector and the different business models. (...) So you need to look at banks, you need to look at education, agriculture, all those attributes that potentially are running, and you need to include them".* Next to the above mentioned perceived challenges with the creation of the European Digital Wallet, Expert H points out that timeline for obligatory development of the eID cards in Member State is the biggest challenge.

Summarized results of the factors identified in Belgium during primary source collection can be seen in Table 3.

Table 3 Factors that affect enactment of cross-border eID in Belgium

Factor dimensions	**Belgium**
Technological factors	*Existence of the unique and persistent identifiers*
	Missing cross-border data interoperability
	Existing Federal Authentication Service
	Legacy system
	High security level of assurance
Organisational factors	*Different approaches towards unique personal identifiers*
	Lack of trust mechanism
	eID was developed for national purposes
Institutional factors	*Limited eIDAS framework focus and success*
	Mobile government trends
	Political effect, digital transformation, COVID 19
Approaches towards new eIDAS proposal on European Digital Identity Wallet	*Positive about SSI European Digital Identity development*
	Hesitant towards the proposed governance of the European Digital Identity development

6.2 Estonia

6.2.1 Technological factors

Existence of the unique and persistent personal identifier

Importance of the existence of the unique personal identifier and its data interoperability is mentioned by several interviewees (Expert A, Expert B and Expert C). The existence of the unique personal identifier is perceived as a main driver but also a challenge for successful cross-border eID. The existing factor of the persistent and unique personal identifiers for technological systems is also supported by the Aavik and Krimmer (2016) Hinsberg et al. (2020).

The importance of the unique and persistent unique personal identifier can be seen in situations of identity and record matching situations.

Identity matching situations happen in order to assure that chosen dataset belong to the correct entity. Identity matching is a challenge for interoperability and identifying people due to the different databases and datasets that are collected by different sectors to identify people (Leosk et al., 2021). This, in turn, results in often inability to automate the decision of identifying people with full assurance. Identity matching is a challenge for national and also for cross-border situations (Leosk et al., 2021). In the case of cross-border situations, identity matching presents a barrier to achieve cross-border recognition of eIDs of other MS. It is agreed that this happens due to the fact that some MS are having different approaches towards unique personal identifiers or not having them at all, according to Expert A. Furthermore, because of these situations, there is a need for a unique personal identifier as "*unique personal identifier should be base for interoperability",* according to Expert A. Also, Expert A states that although some countries are negating the existence of the unique personal identifier, and that "*there is no system that works without identifying uniquely".* In addition, Expert B believes that the existence of unique and persistent identifiers *"will actually make the automatic matching process easier if all the identifiers from each country will be unique and persistent in time".*

Similar to identity matching situations, record matching presents a challenge for identification and authentication across borders. Record matching challenge situations happen due to the fact that the identity of the person is not just their name, surname and birth date. But they also have other attributes that are needed to provide specific service. Sharing these attributes for the purpose of correct identification is perceived as a challenge by Expert A, B, C and D. The solution to overcome the record matching issue and to automate the process, *"even private sector haven't succeed with it"*, according to the Expert A.

In the case of a cross-border situation, the record matching issue happens due to the minimum data sets that are addressed by eIDAS regulation does not fulfil all necessities for all needed attributes to uniquely identify an entity (Leosk,2021). This inability to share attributes across borders is perceived as a big problem mainly because of the heterogenous approaches towards the unique personal identifiers and its interoperability. According to Expert A "*this is a big issue, the unique identifier interoperability for record matching"*.

Central authentication service

Another technological factor that is perceived as one of the drivers for the enactment of the cross-border eID in Estonia is the existence of the Central Authentication Service. The Central Authentication Service enables central gateway of login services for online government services.

According to Expert D, the Estonian success factor was that all online services were consolidated in one single login experience. Expert D mentions, "*More generally, I think the thing that's helped in the public sector is in the last couple of years, the Estonian public services have finally consolidated their logins into a single login service".*

In addition, this Central Authentication Service helped Estonia to integrate the eIDAS functionality to all government bodies. According to Expert B, "*we built a central Authentication Service that helps to integrate the eIDAS functionality to all government bodies and their information systems.".*

Next to creating the Central Authentication Service, Estonian existing eID infrastructure helped to easier implement eIDAS regulation and cross-border eID. Thus, Expert C, mentions that "*the existing starting points and existing infrastructure and solutions definitely helped to, to smoother implementation of the eIDAS and, and we did already have a strong eID solution Estonia deployed and that is being mandatory to use*.".

However, one of the challenges associated with this central authentication service is that it is used only for public sector services. Expert D, mentions "*and I can say from a private sector perspective that's wanted to do for some projects in cooperation with the public sector, to set up its own connection to the eIDAS gateway. Basically, we're told that's not possible right now. So the whole framework, it's, you know, it's only possible for public sector entities".*

Legacy systems

Another important technological factor that was addressed by the interviewees from Estonia is the factor of existing legacy systems. Legacy systems have every country in the EU; thus it can also be a barrier for successful implementation of the cross-border eID in the EU.

The legacy system influence can be seen mainly in cases of cross-border situations. For example, in cases where there are existing unique personal identifiers among two countries, Belgium and Estonia. Both countries have their own unique and persistent personal identifiers. However, these identifiers are not coded in the same way. Estonian e-services were built in 2000, and an integral part and critical infrastructure is the eID and its unique personal identifiers for all entities. Thus, all e-services in Estonia depend on the exact match and algorithm of the unique personal identifiers of Estonian entities. As noted by Expert A, " (…) *and usually our systems local systems in Estonia eID was built in the early 2000s. So our systems are usually built in such a way that the algorithm of this unique identifier is hardcoded in the system, so entering any other number sequence doesn't go in because the system refuses to, saying that this is this is not the correct sequence. And why is this is Estonian legacy"***.** Consequently, any Belgian unique personal identifiers would not be recognized in the Estonian system due to the hardcoded in the system in the 2000s. Another example is that in some Nordic countries, the system does not request birthday dates because the system can automatically recognise birthday dates from the unique personal identifier.

However, Expert A, C and D mention that "*legacy is a local problem*" (Expert A) and that "*this is like a country-specific problem with the Estonian identifier and issuing unmatching the persons with coming in with a different identifier"* (Expert C). In addition, Expert B states that "*although we will have a unique identifier coming from every European Union country to our systems, we still need to provide them with some kind of national a unique identifier.".*

Data interoperability

Data interoperability of unique personal identifiers and data exchange infrastructures are perceived in addition to the existence of the unique and persistent personal identifiers for the IT system as one of the main barriers but also perceived as a driver for proper and accurate exchange of identity data in Estonia, and also for the cross-border eID.

The issue with record matching and identity matching is mostly associated with lack of data interoperability, according to Expert A. During the creation of the eIDAS, proper focus on data interoperability of different attributes was missing. According to Expert A *“this (data interoperability) is this is like a first step that actually should have been done together with the eIDAS regulation”.*

In many use-cases, there is a need for sharing data among different sources and databases. In many cases for cross-border situations of providing e-services, the services are not fully automatic but request additional document or evidence to confirm authentication. Expert A gives an example of the possible use case:

“As simple example, so when I enter the service, online service, again, shouldn't bother me to ask me, okay, please submit your evidence says that you are taxpayers where make your tax declaration from any EU country, submit it, and then what's happening, it is going to be a manual procedure. This is not online service anymore. It's on my channel just to connect to the service, but it's not online. So it's online services that the computer gets the data, validates it and gives result straight away less than a second.”

Furthermore, data interoperability is also an integral part of electronic identification and authentication processes. For example, Expert A states that there is no data interoperability infrastructure across borders to enable automatic service provision. According to Expert A, *“So in this case, when I as Estonian want to log into the other countries portal or somewhere, then this portal should be able to automatically send request to my country's database because they don't have the data about me*”.

One of the main challenges in the data interoperability for cross-border eID, technically, is non-existing cross-border data interoperability infrastructure. This cross-border infrastructure should enable a once-only principle across different domains in the EU. In the EU there are many domain-specific cross-border data exchange pilot projects like tax authority to tax authority, according to the Expert A. However, in many cases of life events and situations, Expert A states:

“But if you think about life events, the services online for life events. Let's say A child is born, you need to register the child, you need to register his name, you need to put in the school to kindergarten that take, preserve that place in kindergarten. It's not just that you are in the one domain, you have to make Aquarius to population registry, you have to make a query to local educational institution, you need to hospital query to population registry to tax authority, and so on. In cross-border situations you need to make queries in his home country. So this is the data interoperability we're talking about.”

In Estonia, existing data interoperability infrastructure created as a basis for data exchange trust, X-Road, is perceived as key enabler for the success of their eID system, according to Expert B and C. However, currently in the EU and for cross-border e-services, "t*here is a lack of privacy control, there is a lack of data trust or source trust, there is no data interoperability that is exchanging the raw data instead of documents.",* according to the Expert A.

High level of security eID schemes

Another technological factor that affects the enactment of the cross-border eID is the high level of assurance. This comes up in situations where Estonian e-services are classified under the high-security trust services by requiring high-security solutions for identifications. Thus, creating an ecosystem that cannot be used by the eID solutions with a lower or substantial level of assurance, according to Expert D.

In addition, Expert B agrees with the opinion of Expert D and states that "*eID notification process and the levels of assurance, this is sometimes a blocker when a country notifies a scheme with a lower level than set, then high of the level of assurance by eIDAS*.".

This situation of a high level of assurance disables the eID schemes from other countries that have low or substantial levels of assurance. As Expert C mentions "*this means that, as Estonian eID means are notified on the level of assurance high, we are not obliged to accept lower than high levels of assurance by other countries. So this means that that the countries who don't have eID at all or who have a lower level or substantial level, they cannot access to our services*".

The inability to accept other eID schemes with low or substantial level of assurance, is associated with the system requirements of the e-service providers in Estonia, according to Expert B.

6.2.2 Organisational factors

Approaches towards cross-border eID

Approaches towards unique personal identifiers can vary, from being handled as public data or secret data, to having multiple personal identifiers for specific use.

In Estonia, a unique personal identifier is perceived as a base for interoperability of its e-services, in addition to Estonian data exchange system X-Road (Expert A, B and C).

According to Expert A, unique personal identifiers should be handled as public data. During the interview, Expert A mentioned that "*unique identifier must be something that* *is must be considered as a public data. I not saying it's a public data, but it has to be handled as a public data*.”. In Estonia, the use of unique personal identifiers is allowed to everyone, private or public services who have joined and who have been accepted to their data exchange trust framework X-Road.

Furthermore, in some countries, unique personal identifiers are handled as protected data due that it contains identity data which can limit the privacy of entity. This problem is addressed by Expert A, who says, “*so what I see that some countries do big mistakes they are, they are say they have this unique identifier, but they don't allow to use it outside their own system.”* This unwillingness to share unique personal identifiers present a barrier for cross-border eID.

Also, usually when the unique personal identifiers are seen as protected and not handled as a public data, it is used as an access key that is used by some system designers. This is the reason because it contains data that only government and each entity should know. Due to the fact that it is used as an access key, it cannot be kept in secret, and it can be accessible on the internet. An example of this situation gave Expert A, *“Exactly what we see in the US happened with a social security number, because this is secret. And this only something person knows and government knows. So if you want to get access over a phone line, what is the access key or recover key? Well, easiest is something only this person knows nobody else.”.*

Next to the unwillingness to share unique personal identifiers to other systems, some MS have the approach that has different unique personal identifiers for the physical environment and for electronic services environment, *“some countries, they don't have a number and now they create it and this is used only an electronic services”*,according to the Expert A. In the case of cross-border data sharing, due to the privacy, some countries even create new identifiers for their citizens, “so *for cross border transactions, some countries they have maybe some number for physical services and some for electronic services.”,* according to Expert A.

The barrier with multiple provision of personal identifiers can be seen in cross-border situations and an example of record matching issues in the system. Expert A gives an example of the situation: “*In the passport you are in ID card you have one number that is unique identifier and in your eID different, your country are not sending the same number to other country. They are creating completely new numbers saying that this is that entity and then let's do it cross border. And what's happening? This is a classic example of record matching issue.”.*

In addition, Expert B mentions that "*we don't know how the other countries have and will provide their attributes and whether they whether they are attending or what is the their process it might be totally different from our perspective, we share a lot of data about our persons but some countries are very strict about it"*.

Trust mechanism

The existence of the trust framework and trust mechanism for exchange of identity information among authoritative sources is necessary, according to Expert A. It is essential to create a trust governance both for identity information and for data exchange infrastructure.

One of the main trust sources for data exchange and eIDs are the authoritative sources. These authoritative sources are the basis of trust because these sources hold the original data. It is "*the source where you have this original data"* (Expert A). Furthermore, the issue with trust in the cross-border situation is even more significant. Expert A states that *"the problem with this (sharing identity data and attributes) is that one country doesn't trust another country because we don't know if behind this hub (source) are some private sector companies, maybe this is a fake web page who is trying to just fishing the information".* Consequently "*there has to be some kind of trust mechanism"* (Expert A).

Moreover, creating some kind of trust framework for sharing unique personal identifiers is important especially in cases of sharing privacy information such as identity data. Thus, if *"there is no trust model between the countries nobody wants to use it"*, according to Expert A.

Human resources

The number of human resources that are involved in the topic of digital identity is seen as a limiting organisational factor. In addition, due to the fact that Estonia is a small country *"human factors become more relevant when you're just dealing with small numbers of people."*, according to the Expert D. In addition, Expert C also agrees with Expert D, by saying that *"one of the problems that we already talked this week that Estonia, is that we have a small community, on the field of eID"*.

Lack of human resources also have an effect on the participation on European projects and initiatives. Expert D, mention that "*it also means that you are not able to take part of all the initiatives in European level, you cannot be everywhere, and that there is a lack of expertise in different projects where you may be should put your time more. So this is actually something we know".*

However, it is also perceived as a positive factor due to the fact information and data can be exchanged fast. According to Expert C, *"it is very good that we have this kind of, you know, we can exchange information very fast. And there are no many people, you know, that you have to find, and talk and so on."*.

Furthermore, this finding is in line with Aavik and Krimmer (2016), who also recognized the lack of human resources as significant limiting factor.

6.2.3 Institutional factors

Limited eIDAS framework focus and success

Opinion regarding of the current eIDAS framework is that its primary focus is on public sector while neglecting private sector providers or services. According to the Expert D, "t*he whole framework, it's, you know, it's only possible for public sector entities."*. The private cross-border company is unable to connect to the eIDAS nodes and provide services through central authentication service, according to Expert D.

The implementation of the eIDAS nodes are not evenly distributed. There is not enough countries in the EU who have implemented eIDAS nodes to enable cross-border identification and authentication electronically, according to Expert D. Currently, only nine MS have successfully and fully implemented eIDAS nodes in their countries (Eurosmart, 2020).

Another factor is that "*eIDAS is just a half of the equation*", according to Expert A. This is the case because to enable seamless cross-border eID in the EU, once-only principle and data interoperability is required. Hence, Expert A claims that "*they should have data interoperability as a trust service as well."*.

Also, it is perceived that there is no clear incentives towards participation to the cross-border enactment by the private sector. Mainly, Expert D states "*Because the eIDAS is so specifically about recognising identity for logging into public sector services between countries*. T*here's not an economic component to it at all. It's provided for free public, the public sector."*.

Approaches towards e-identity management

"*Identity itself, or core identity, it has to be conservative*", Expert A stated. This is addressing the approach of institutions towards core identity and identity management. In Estonia, eIDM are based on centralized approach where identity is provided only by government in cooperation with the private sector.

Conservative or centralized approach is that government identifies people and its citizens, by giving them ID cards or driving licence. These evidences are from authoritative sources that is trusted and "*this is an evidence from the government that this is we have identified you, and this is evidence that you are you as a government knows you*" (Expert A). Thus, the same should work also for online services.

Approach that is used in the USA as market based approach or UK where there is identity is considered as self-sovereign, for example, electric bill can be used as identity document. Thus, Expert A claims that "*this has to be the same conservative. The way of thinking like they do in the US that let the market solve it and let the banks and everybody identify you. It doesn't work here".*

Main reason why e-identity should be provided only by governments issued documents are because market based approach is too risky and also it "*cannot make a fully automated services build on that actual time"*, according to Expert A.

In addition, the institutional perspective of Estonia towards unique personal identifier is that, those identifiers are considered as public data. One of the main reasons for that is because nowadays it is easy to find on the public accessible internet. *"Pandora Box is open"* (Expert A), thus it should be handled and perceived as a public data.

6.2.4 Opinions on the Proposal and European Digital Identity Wallet

Through interviews, participants were asked to provide their opinion on the new eIDAS proposal for eIDAS amendments and creation of the European Digital Wallet, proposed on the 3. June 2021.

In Estonia, there is a potential concern towards the development of the European Digital Wallet based on self-sovereign identity. Expert A states that the proposed changes on creation of the self-sovereign identity can be good to solve the problem of attribute sharing and data interoperability. More specifically, "*self-sovereign identity is pretty good to solve this issue where we talk about that we don't have data interoperability*." (Expert A).

However, the bigger concern is towards the citizens being a data carrier or data exchange layer. According to Expert A, "*it's basically copying the model we have in the physical world, if you want to take, let's say, you want to establish a company in these countries who doesn't have a service for that, while you're doing, you're going to one, taking papers, you're running with these papers to another institution, they get the stamps there, then you go into the third. So you are data carrier, you are data exchange layer, and the same thing happens with self-sovereign identity".* The reason why it is problematic for the user to be a data carrier is because of security and risk reasons. Due to the fact that all personal data (evidence) are kept on the mobile phone, there is a high risk for data to be exposed, according to Expert A.

Next to the security issues, important is the trust model that is existing with the proposed European Identity Wallet. Attributes change over time, for instance, you can be a student in one period of time, and then status being revoked. By being a data holder of the certified evidence provided by authoritative sources, it can be hard to assure the validity or actuality of the existing authoritative sources. Expert A gives an example: "*You can have your university diploma. One thing is to check is it still valid or dismissed. But another thing is that how we can trust or we know that the University exists, we know that this is authoritative source, how we know that this is not being recalled or anything.".* Additionally, "*the problem is that you are not trusting origin source, you are trusting the person's wallet, and you don't know where this information came to this wallet, yes, if it's a sealed sign, you can check the signatures and things. But you are not, you don't know if it's still valid. In time, things can change.".*

In addition, Experts A, B, C agreed that the new eIDAS proposal would not solve all problems. Expert B stated, *"I think the digital wallet, European wallet identity solution will not improve will not provide the solution for everything.".* Also, Expert B and C agreed in the opinion that "*this digital wallet can be a solution for those countries who have been not successful so far in the eIDAS implementation*" (Expert B).

Furthermore, interviewees expressed worries about possible required changes in procedures if instalment of the European Digital Wallet will be compulsory. Expert C mentioned that "*it (new eIDAS proposal) means that it also creates kind of new situation, and also maybe some additional burden to that, for those countries who actually have already quite well-developed systems in place.".*

Finally, it is important to note that the interviews were held shortly after publishing the proposal. Hence, interviewees were cautious in giving their opinion due to undeveloped and unpublished parts of proposals such as, inter alia, technical standards and implementation plan.

Summarized results of the factors identified in Estonia during primary source collection can be seen in Table 4.

Table 4 Factors that affect enactment of cross-border eID in Estonia

Factor dimensions	**Estonia**
Technological factors	*Existence of the unique and persistent identifiers*
	Missing cross-border data interoperability
	Existing Central Authentication Service
	Legacy systems
	High security level of assurance
Organisational factors	*Different approaches towards unique personal identifiers*
	Lack of human resources
	Lack of trust mechanism
Institutional factors	*Limited eIDAS framework focus and success*
	Approaches towards identity management
Opinion on European Digital Identity Wallet	*Concerns towards user-centric eIDMS*
	Resistance towards technical implementation of European Digital Identity Wallet

7 Discussion and recommendations

7.1 Discussion

In the previous chapter, identified factors derived from data analysis of the primary source collection were presented. Table 2 and Table 3 present the summary of identified factors that affect the enactment of the cross-border eID in Belgium and Estonia. However, due to the objective of this research and its research questions, it is highly important to discuss the findings and their respective factors between Estonia and Belgium.

On the part of the technological factors, it is identified that one of the most important factors with a positive impact is the existence of unique personal identifiers. Both countries have emphasised their unique and persistent personal identifiers as an important driver towards the enactment of the cross-border eID. In Estonia, this identifier is called a personal identification code, while in Belgium national register number. However, these identifiers are different between the two countries. For example, the formation of these UPI is done in a different manner. Also, as stated in the results, the IT systems of both countries are depended on the sequence of the identifier. Hence, the existence of unique and persistent identifiers are found as a crucial aspect in the success of eID systems in both Belgium and Estonia, and that also improves enactment of the cross-border eID. These differences and choices towards its existing unique personal identifiers cause a lack of cross-border eID success because it cannot be used in other IT country systems. Thus, this finding confirms, the existence of unique and persistent personal identifiers further refine organisational settings and legal framework towards cross-border eID. Furthermore, in both countries existence and creation of the central authentication service is found as an important driver which consolidated a single authentication gateway for citizens and businesses. Centralization of the single authentication gateway in one central authentication gateway enabled both Belgium and Estonia to have a successful eIDAS nodes implementation and enabled cross-border eID. Also, it is interesting finding that approach towards centralization of the authentication system has been perceived as a driver in both centralized Estonia and federated Belgium.

Legacy systems existing both in Belgium and Estonia is perceived as a technological factor that has negative but also positive impact. Both countries have developed strong eID infrastructure since the beginning of the 2000s. This affects the organisation and policy towards cross-border eID. Unwillingness to change existing infrastructure and hesitance towards the changes of technology and legacy that is functioning well for national e-services has been noticed. Also, in both countries, existing infrastructure and their experience towards eID has been seen as an important driver for the smooth implementation of eIDAS nodes and enabling cross-border eID.

Another important technological factor that is affecting the enactment of cross-border eID is the lack of cross-border data interoperability systems in the EU. The cross-border data interoperability systems are still underdeveloped in the EU, and it affects the sharing of additional attributes and credentials for proper identification and automation of the e-services provision. Although, nationally, in both Estonia and Belgium once-only principle is successfully implemented, which enables a seamless exchange of data, which is not the case for cross-border e-services. Thus, the lack of proper cross-border data exchange infrastructure and cross-border once-only exchange of data affect the successful enactment of the cross-border eID. The inability to share relevant data affects data interoperability for cross-border eID. The lack of existing data interoperability infrastructure for cross-border causes record matching issues (Leosk et al., 2021). The record matching issues are identified as one of the most crucial problems with cross-border eID enactment in both case study countries.

Finally, another limiting technological factor towards the successful enactment of the cross-border eID in the EU is the requests for a high level of security assurance. The high-security requirements for eID schemes and their trust services have been perceived as limiting factors for further success of the enactment of the cross-border eID. Due to the fact that service providers in Estonia and Belgium often require high-security level of assurance, it affects the most often usability of other eID means in the country. To put it more simply, it affects the usability of the eID means for cross-border eID. For institutions and organisations, it is important to have high secure eID schemes. Thus the policy decision affects the technology design of the eID schemes and their usability in cross-border settings.

On the organisational part, the most important organisational factor that limits the cross-border enactment is different approaches of countries and their organisation towards personal identifiers. Both case study countries have unique and persistent personal identifiers but different legal and organisational approaches. In Estonia, a unique personal identifier is handled as public data and is allowed to be used and accessed by other organisations inside and outside the country. While in Belgium, the national registry number is considered as protected data and is not allowed to be used outside the public sector and by foreign administrations. Moreover, in some other MS, there are approaches towards many personal identifiers for different sectors, or there is the non-unique and persistent identifier in the country. These different national policy choices, approaches and decisions towards the design and use of identifiers negatively affect the interoperability of data and cross-border eID success in the EU. This finding is confirmed by the validation interview expert who mentioned that "*you can indeed see, though, these are the choices that you've made as a Member State, which make your life easier or harder, at least from a functional perspective, not saying that the outcome necessarily is better for citizens or worse for citizens. But at least for the interoperability part.".* Furthermore, the organisational agreements and arrangements at the EU level for identity data and credentials interoperability are necessary. Further cooperation and the creation of a governance trust framework of authoritative sources in countries is necessary. Since there is still an unwillingness and lack of trust for the cross-border data exchange and its attributes, organisations cannot properly identify and provide seamless and automatic e-services to all EU citizens. Lack of human resources that are involved in cross-border eID in the organisations is perceived as one of the limiting factors in Estonia. In Belgium, human factors were not mentioned as a factor towards the enactment of the cross-border eID. One of the reasons why this is a case can be because Estonia has a small population while Belgium has a bigger population and EU is considered as EU centre.

Finally, a difference that is existing in Belgium and Estonia in organisational aspects is the involvement of the banks and telecom operators which can improve the use of eID also for cross-border settings. With the involvement of Banks and telecom operators, as one of the main actors in eID development in Estonia, enabled the various use of e-services also private services. While in Belgium, bank and telecom operators were involved in the provision of eID schemes "it's Me", almost 15 years after the creation of eID cards, which resulted in higher identification and authentication processes by citizens. The factor of involvement in the organisation of banks and telecom operators is also confirmed by the validation interview expert. Expert J, mentioned "*In Belgium, things started taking off when they started using mobile identification, because it was a smartphone app. And also because it was used by banks. So you can do your home banking with your eID. And that looks a lot better.".*

From the part on institutional factors, a limited eIDAS regulation has been recognized as a driving but also limiting factor. The eIDAS regulation and its minimum dataset requirement, rigid and complex notification processes have been considered as a reason for the lack of cross-border eID enactment in the EU. In addition, the lack of involvement of other stakeholders and private actors in the creation process of the eIDAS framework was perceived as a barrier to the full success of eIDAS regulation. This finding was confirmed by the validation interviewee, who stated that "*the problem with the European identity infrastructure is that it's very limited in terms of the identity information that it can support. But what it doesn't do as it needs to the more innovative stuff like to let you* *add credentials or attribute assertions, attribute statements, certificates and evidence documents, let you add that to your identity*".

Another institutional factor that limits the development of the cross-border eID enactment is the different philosophy towards identity. Estonia perceives that identity management and identity data sharing should be managed by the government. During the validation interview, Expert J confirmed this finding by stating that it can be seen an influence of the centralised philosophical approach towards identity in which government is responsible for the provision of identity and control of identity data. However, Estonia is to some extent, hesitant towards user-centric identity management, which is becoming more popular with mobile identities and SSI. While in Belgium, there is a high number of SSI projects and initiatives towards mobile identities and user-centric identity management models. It can be seen that this approach towards new technology, eID, is affected by the ideological and institutional culture in a way where eID is perceived as a government responsibility.

Finally, the COVID-19 pandemic has been perceived as a driver for digital transformation and cross-border eID. Due to the pandemic situations, many governments have acknowledged the necessity of the e-services and the drawbacks of current e-government development. Furthermore, the importance of cross-border e-services has been emphasised throughout the EU. This stems from the fact that many countries have closed borders, which caused many citizens to be unable to access to public administration services.

New eIDAS amendments proposal and European Digital Identity Wallet

During the interviews, as part of this research, interviewees were asked to provide their opinion and insights on a newly published proposal for the amendments of eIDAS regulation and proposed European Digital Identity Wallet. It is found that in Estonia, scepticism and resistance exists towards the SSI model and its creation of the European Digital Identity Wallet. Mainly in Estonia are concerned about the security of the user-centric e-identity management model used in SSI. Hence, main comments were addressed towards the technological solutions and possible negative scenarios that might be caused by the user-centric identity management model. This expectation is in line with the institutional view towards identity, which is perceived that the e-identity management and e-identity data sharing would be under government control. Furthermore, in Estonia it is believed that new eIDAS proposal might cause unnecessary changes in their already developed eID ecosystem by making obligatory development of the European Digital Identity Wallet. This requirement is seen as a positive thing that will incentivise other MS to develop their eID solutions; however, as already mentioned in Estonia exists scepticism towards the European Digital Identity Wallet. Similarly, the validation interviewee Expert J also agrees on the point of the concerns towards user security and the responsibility of the governments towards the SSI and use of the blockchain technology. Expert J also says, "*I think for a lot of governments, a lot of public administrations, the business case for blockchain is unproven. The benefits for them is unproven. I think that's that is a challenge as well*."

Conversely, in Belgium, there are positive expectations towards SSI and European Digital Identity Wallet. One of the reasons might be because Belgian institutions at regional and local levels are piloting projects that employ SSI and blockchain development. Furthermore, the positive view on the creation of a new European Digital Identity Wallet is also in line with the perspective towards the development of the mobile identity and paradigm shift from e-government towards the mobile government. Belgium recently have accepted mobile private eID means "it's Me" to improve the use of e-services, and found that there are need for a shift towards mobile government and mobile identities with sovereignty on the side of the citizen. However, there are some concerns and expected challenges that are existing with the new eIDAS proposal. The main concerns over the new eIDAS proposal are focused more on the governance model and how interoperability governance will be achieved. Mainly, due to subsidiarity creation of the European Digital Identity Wallet is mainly the responsibility of the Member State, hence, it might happen that the focus is again on national e-services while neglecting cross-border interoperability. Furthermore, lack of stakeholders involvement and focus only on the public sector is seen, again, as a future challenge. Due to these concerns, it is expected that the main problem that is trying to be solved, which is cross-border interoperability and mutual recognition of eIDs, will exist again even after the new eIDAS proposal and the creation of the European Digital Identity Wallet.

Summary and comparison table with the identified factors show the commonalities and differences that are existing between Estonia and Belgium with the cross-border eID enactment in the EU (see Table 5).

Table 5 Comparison table on the commonalities and differences between Estonia and Belgium

		Commonalities		**Differences**	
Dimension	**Discussed factors**	**Estonia**	**Belgium**	**Estonia**	**Belgium**
Technological dimension	**UPI**	*Existing UPI*		*Personal Identification Code*	*National Registry Number*
	Central authentication service	*Existing central authentication service*		*Central Authentication System*	*Federal Authentication System*
	Data interoperability	*Lack of cross-border interoperability*		*X-Road*	*Federal Service Bus*
	Level of assurance	*High level of assurance of eID schemes*		-	
Organisational dimension	**Approach towards UPI**	-		*UPI handled as public data*	*UPI handled as protected data*
	Trust mechanism	*Lack of cross-border trust mechanism*		-	
	Access to private services	-		*Access to private services*	*Lack of access to private services*
Institutional dimension	**Approaches towards identity**	*Centralized approach on government identity management*		*Government control on identity management and use*	*Sovereign identity management and use*
	eIDAS regulation	*eIDAS perceived as limited*		-	
European Digital Identity Wallet	**Approach towards user-centric identity model**	-		*Sceptic about user-centric model*	*Positive about user-centric model*
	New eIDAS proposal	-		*Focus on technological challenges*	*Focus on governance challenges*

7.2 Recommendations

In this section of the research, recommendations suggested by interviewed experts and by the author of this research are presented. Recommendations on overcoming the existing factors that present challenges and how to improve cross-border eID enactment are classified if they are up to national responsibility or the EC responsibility. Thus, existing challenges should be overcome by joint action and cooperation towards unifying national policies in the eID field.

Existing challenges that are identified in this research could be overcome on the national level by following actions. First, different approaches of MS towards the existence of UPI and handling of UPI affect the cross-border eID enactment and mutual recognition of eID schemes. Thus, the recommendation is that MS could align approaches by agreeing on common standards of handling the UPI on a cross-border level. Moreover, as the existence of a central authentication portal was identified as a factor with a positive impact on cross-border eID enactment, MS might design common policies towards a unified single sign-on experience for cross-border users.

Factors that fall under the EU level competencies, which can be overcome by EU level involvement, could be overcome by following actions. Experts identified a need for increased and intense European collaboration for enacting the cross-border eID. Thus, Interoperability governance could be considered at the EU level and by MS with promoting and utilizing the existing European Interoperability Framework. Furthermore, it is acknowledged that there is a lack of involvement of relevant stakeholders in the policy creation process at the EU level. Hence, the involvement of relevant private sector and public sector stakeholders could help to overcome existing challenges. Another recommendation that is suggested by the experts was the creation of the identity hub on the EU level. The identity hub would contain a unified UPI and enable record matching and identity matching process. Finally, developing and updating cross-border data interoperability infrastructure on the EU level is considered an important step in how cross-border eID could be achieved.

8 Conclusion

Identifying people by reciting Whakapapa like in Maori culture is no longer a common practice. Nowadays, the identification of individuals is conducted through identity documents that the governments and central authorities provide. Moreover, with the development of the internet society and electronic government, previous identification practices have become obsolete. Thus, governments developed electronic identities to enable citizens to access online services. However, at the beginning of creating eIDMS, many countries have independently focused on developing eIDMS only for national purposes. For citizens and businesses in the EU, this created an additional burden of having multiple and non-interoperable eIDs and the inability of public administration to identify cross-border public e-services users.

Consequently, independent approaches towards eIDMS have resulted in heterogenic systems of eIDMS in the EU. This heterogeneity of eIDMS at the EU level causes a low level of eID interoperability, which is necessary for the achievement of the EU Digital Single Market goals. Thus, the purpose of this research was to explore factors that affect the cross-border eID enactment from a national perspective. Utilizing a case study approach, Estonia and Belgium had been chosen, as digitally advanced countries, with the purpose to find commonalities and differences existing in the cross-border eID enactment. Furthermore, this research discussed the perspectives of Estonia and Belgium on the new European Digital Identity Wallet.

This research aimed to answer the central question: "*What factors affect the cross-border eID enactment in the EU from Estonian and Belgian perspectives?".* The following sub-questions were addressed with the purpose to answer the central research question: *"What are the perspectives of Belgium and Estonia on new eIDAS proposal and European Digital Identity*?"; "*What are the recommendations to overcome identified challenges?".*

EU institutions and MS have been creating cross-border initiatives and developing policies to enable cross-border Digital Single Market. eID is considered one of the most important enablers for mature e-services. However, in the EU, at least 3% of its population is considered to be commuting across borders and for that population, there is no possibility to use nationally issued eID for e-services in a destination country in the EU. Hence, throughout this research, primary and secondary data collection, as well as thematic data analysis, were conducted by interviewing eleven experts in the cross-border eID field and through NVivo software. Classification of the factors was done based on the theoretical framework, the Technology Enactment Framework.

Results show, in both Estonia and Belgium, that technological factors are similar. Factors that are identified in data collection demonstrate the importance of the existence of the UPIs; unified authentication service system. Impact of the legacy system, lack of cross-border data interoperability infrastructure and high-security level of assurance requests are identified as factors that have a significant impact on cross-border eID. However, some differences are found on the part of organisational factors between Estonia and Belgium. In Belgium, the organisational approach towards sharing UPIs is rather restricted, while in Estonia, UPIs are handled as public data. In regards to the involvement of stakeholders, Belgium has not involved banks and telecom operators from the beginning of eID development, while in Estonia, banks and telecom operators were important actors in the eID ecosystem since 2002. However, both in Estonia and Belgium, it is acknowledged that there is a lack of cross-border trust mechanisms in the eID field. Regarding institutional factors, existing eIDAS regulation is perceived as limited, both in Estonia and in Belgium. Furthermore, there is a possible distinct approach towards e-identity management perspectives and approaches in development. In Estonia, the existing perspective is that the possible wanted scenario of e-identity management and identity data sharing would be managed by the government. On the other hand, the existing perspective in Belgium is that e-identity management and identity data sharing would be sovereign and in control of the user.

Regarding the new eIDAS proposal and proposed European Digital Identity Wallet, Estonia and Belgium have, to some extent, different perspectives. Estonia is being concerned with technological solutions that European Digital Identity Wallet provides and is simultaneously concerned with the security characteristics of SSI. On the other hand, Belgium has been positive about European Digital Identity Wallet and mobile identities, while more concern was expressed on future interoperability of identity wallets and development coordination in the EU. Furthermore, when it comes to e-identity management and identity sharing, in Estonia, it is found out that scepticism exists towards user-centric identity data control and security of identity data. In contrast, a positive approach towards SSI development can be found in Belgium. This is in line with more focus in Belgium on mobile identity sovereign management as a more preferred future option.

Another objective of this research was to provide recommendations on overcoming existing challenges in cross-border eID enactment. Recommendations proposed in this research are classified as recommendations for the national level and recommendations to the EU level. Firstly, MS in the EU may consider developing and providing UPIs to their citizens and could work on developing a unified single authentication service for improved user-experience of cross-border users. Furthermore, Member States could work on aligning policies towards common standards of identity data sharing across borders. On the EU level, one possibility is to include more stakeholders from relevant sectors of identity management in the policy-making processes. Another recommendation was addressing the possibility of improving the existing cross-border data interoperability infrastructure. Last but not least, the creation of an identity hub at the EU level could be a part of the solution for solving the challenges of record matching and identity matching issues.

References

Aavik, G., & Krimmer, R. (2016). Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In H. J. Scholl, O. Glassey, M. Janssen, B. Klievink, I. Lindgren, P. Parycek, . . . D. Sá Soares (Eds.), *Lecture Notes in Computer Science. Electronic Government* (Vol. 9820, pp. 151–163). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-44421-5_12

Aichholzer, G., & Strauß, S. (2010). Electronic identity management in e-Government 2.0: Exploring a system innovation exemplified by Austria. *Information Polity*, *15*(1,2), 139–152. https://doi.org/10.3233/IP-2010-0203

Alonso, L. B. (2021, April 21). *A future for eIDAS ?* DigiALL Public Conference,

Andrade, N. N. G. de (2012a). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, *28*(2), 153–162. https://doi.org/10.1016/j.clsr.2012.01.012

Andrade, N. N. G. de (2012b). Towards a European eID Regulatory Framework. In S. Gutwirth (Ed.), *European data protection: In good health?* (1st ed., pp. 285–314). New York: Springer. https://doi.org/10.1007/978-94-007-2903-2_14

Andrade, N. N. G. de, Chen-Wilson, L., Argles, D., Wills, G., & Di Schiano Zenise, M. (2014). *Electronic Identity*. London: Springer London. https://doi.org/10.1007/978-1-4471-6449-4

Andrasko, J. (2017). Mutual Recognition of electronic identification means under the eIDAS regulation and its application issues. Retrieved from https://www.researchgate.net/publication/339973932_MUTUAL_RECOGNITION_OF_ELECTRONIC_IDENTIFICATION_MEANS_UNDER_THE_EIDAS_REGULATION_AND_ITS_APPLICATION_ISSUES?enrichId=rgreq-bae282935ecfc4af17e3ef17a55ebce3-XXX&enrichSource=Y292ZXJQYWdlOzMzOTk3MzkzMjtBUzo4Njk5OTczNjY3NDcxMzZAMTU4NDQzNDk0NDI3NQ%3D%3D&el=1_x_3&_esc=publicationCoverPdf

Angelis, F. de, Falcioni, D., Ippoliti, F., Marcantoni, F., & Rilli, S. (2016). Federated identity management in e-government: lessons learned and the path forward. *International Journal of Electronic Governance*, *8*(1), 22. https://doi.org/10.1504/IJEG.2016.076683

Anthes, G. (2015). Estonia: A Model For E-Government. Retrieved from https://cacm.acm.org/magazines/2015/6/187320-estonia/fulltext

Badinger, H., & Maydel, N. (2009). Legal and Economic Issues in Completing the EU Internal Market for Services: An Interdisciplinary Perspective. *JCMS: Journal of Common Market Studies*, *47*(4), 693–717. https://doi.org/10.1111/j.1468-5965.2009.02001.x

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, *13(4)*, 544–559. Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss4/2/?utm_source=nsuworks.nova.edu%2Ftqr%2Fvol13%2Fiss4%2F2&utm_medium=PDF&utm_campaign=PDFCoverPages

Bazeley, P. (2013). *Qualitative data analysis: Practical strategies / Pat Bazeley*. Los Angeles: SAGE.

Belgium (2018). *NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9(5) OF REGU: Belgian eID*. Retrieved from https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Belgium+-+eID

Belgium (2019). *Notification process itsMe.*

Bender, J. (2015). *eIDAS Regulation: eID – Opportunities and Risks*. Retrieved from Bunde.de. Fraunhofer-Gesellschaft website: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/SmartCard_Workshop/Workshop_2015_Bender.pdf?__blob=publicationFile&v=1

(2020). *Berlin Declaration on Digital Society and Value-Based Digital Government: at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020*. Retrieved from Berlin Declaration on Digital Society and Value-Based Digital Government (21-Dec-20). Publications Office of the EU. Retrieved from https://data.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brugger, J., Fraefel, M., & Riedl, R. (2014). Raising Acceptance for eID for cross-border egov. In A. Ionas (Ed.), *Proceedings of the 14th European Conference on eGovernment: ECEG 2014 : Spiru Haret University, Faculty of Legal and Administrative Sciences, Brasov, Romania : 12-13 June 2014 / edited by Alexandru lonas* (Vol. 2014). Reading: Academic Conferences and Publishing International Limited.

Bryman, A. (2016). *Social research methods* (Fifth Edition). Oxford, New York: Oxford University Press. Retrieved from https://www.loc.gov/catdir/enhancements/fy1617/2015940141-b.html

Carretero, J., Izquierdo-Moreno, G., Vasile-Cabezas, M., & Garcia-Blas, J. (2018). Federated Identity Architecture of the European eID System. *IEEE Access*, *6*, 75302–75326. https://doi.org/10.1109/ACCESS.2018.2882870

Cave, J., Botterman, M., Cavallini, S., & Volpe, M. (2017). *EU Wide digital Once Only Principle for citizens and businesses*. Retrieved from European Commission website: https://ec.europa.eu/esf/transnationality/filedepot_download/1671/1692

CEF Digital (n.da). Connecting Europe Facility in Telecom - Shaping Europe’s digital future - European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/connecting-europe-facility-telecom

CEF Digital (n.d.b). eID. Retrieved from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eID

CEF Digital (n.d.c). eIDAS Levels of Assurance. Retrieved from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+assurance

CEF Digital (n.dd). Who is involved in eID? Retrieved from https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773200

CEPS (2019). *Evaluation Study supporting the interim evaluation of the programme on interoperability solutions for European public administrations, businesses and citizens (ISA²): Final Report.*

Crahay, A., Di Giacomo, D., Chloé, D., Ghita, E., & Talpo, S. (2021). *Report on Public Administrations’ Digital response to COVID-19 in the EU*. Luxembourg. Retrieved from European Union website: DOI: 10.2799/085839

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry & research design: Choosing among five approaches* (Fourth edition). Los Angeles: SAGE.

Cuijpers, C., & Schroers, J. (2014). Eidas as guideline for the development of a pan European eid framework in futureid. In D. Hühnlein & H. Roßnagel (Eds.), *Open Identity Summit 2014* (pp. 23–38). Bonn: Gesellschaft für Informatik e.V.

Danziger, J. N. (2004). Innovation in Innovation? *Social Science Computer Review*, *22*(1), 100–110. https://doi.org/10.1177/0894439303259892

De Andrade, N. N. G., Monteleone, S., & Martin, A. (2013). *Electronic Identity in Europe: Legal Challenges and Future Perspectives (e-ID 2020).*

De Cock, D., Wolf, C., & Preneel, B. (2006). The Belgian Electronic Identity Card (Overview. Retrieved from https://www.esat.kuleuven.be/cosic/publications/article-769.pdf

Delos, O., Debusschere, T., Soete, M. de, Dumortier, J., Genghini, R., Graux, H., . . . van Eecke, P. (2015). A pan-European Framework on Electronic Identification and

Trust Services for Electronic Transactions in the Internal Market. In H. Reimer, N. Pohlmann, & W. Schneider (Eds.), *ISSE 2015* (pp. 173–195). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-10934-9_15

Dumortier, J., & Vandezande, N. G. (2012). Critical Observations on the Proposed EU Regulation for Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. *SSRN Electronic Journal.* Advance online publication. https://doi.org/10.2139/ssrn.2152583

E-Estonia (n.d.). e-Estonia — We have built a digital society and we can show you how. Retrieved from https://e-estonia.com/

ESPON (2020). *Cross-border public services in Europe*. Retrieved from https://www.espon.eu/sites/default/files/attachments/7744%20ESP%20Policy%20Brief%2C%20Cross-border%20public%20services_4_web.pdf

European Commission (n.d.a). About ISA - ISA - European Commission. Retrieved from https://ec.europa.eu/archives/isa/about-isa/index_en.htm

European Commission (n.db). Electronic interchange of data between administrations: IDA programme Electronic interchange of data between administrations: IDA programme. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24147a&from=EN

European Commission (2005). Report on the Evaluation of the IDA II programme. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52005DC0493&from=LT

ISA programme (2009).

CEF Programme (2013).

European Commission (2015a). *COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1501&from=EN

European Commission (2015b). *A Digital Single Market Strategy for Europe - Analysis and Evidence: COMMISSION STAFF WORKING DOCUMENT A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe.*

European Commission (2015c). *A Digital Single Market Strategy for Europe: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN*

PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A digital Single MArket Strategy for Europe.

ISA2 programme (2015).

European Commission (2017). Ministerial Declaration on eGovernment - the Tallinn Declaration | Shaping Europe's digital future. Retrieved from https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

European Commission (2020a). Communication from the Commission - Shaping Europe's Digital Future: COM(2020) 67 final.

European Commission (2020b). *Digital Government Factsheet Belgium 2020.*

European Commission (2020c). *Digital Public Administration factsheet 2020 Estonia.*

European Commission (2020d). *eGovernment benchmark 2020: Background report.*

European Commission (2021a). The European single market - Internal Market, Industry, Entrepreneurship and SMEs - European Commission. Retrieved from https://ec.europa.eu/growth/single-market/

European Commission (2021b). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. Retrieved from European Commission website: https://op.europa.eu/en/publication-detail/-/publication/35274ac3-cd1b-11ea-adf7-01aa75ed71a1/language-en

Directive 2006/123/ECOfficial Journal of the European Union (2006).

ESignature Directive 1999/93/EC (1999).

European Union (2014). *eIDAS Regulation (EU) No 910/2014: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. Official Journal of the European Union.

Eurosmart (2020). *Implementation of the eIDAS nodes: State of play*. Retrieved from https://www.eurosmart.com/implementation-of-the-eidas-nodes-state-of-play/

Eurostat (2019). Belgium. Retrieved from https://ec.europa.eu/eurostat/documents/10186/10994376/BE-EN.pdf

Fairchild, A., & de Vuyst Bruno (2012). The Evolution of the e-ID card in Belgium: Data Privacy and Multi-Application Usage. In J. L. Mauri, G. Martinez, L. Berntzen, & Å. Smedberg (Eds.), *The Sixth International Conference on Digital Societ: ICDS 2012*. International Academy, Research, and Industry Association: IARIA.

Federal Government Belgium (n.d.). Digital Belgium : the Digital Agenda for Belgium | FPS Economy. Retrieved from https://economie.fgov.be/en/themes/online/digital-belgium-digital-agenda

Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Washington D.C.: Brookings Institution Press.

Fountain, J. E. (2004). Enacting Technology in Networked Governance: Developmental Processes of Cross-Agency Arrangements.

Fountain, J. E. (2008). Bureaucratic reform and e-government in the United States: An institutional perspective. In A. Chadwick & P. N. Howard (Eds.), *Routledge Handbook of Internet Politics* (pp. 115–129). Routledge. https://doi.org/10.4324/9780203962541-15

Fries-Tersch, E., Jones, M., & Siöland, L. (2021). *Annual Report on Intra-EU Labour Mobility 2020.*

Fritsch, M., & Bertenrath, R. Dr. (2019). *Cross border services in the internal market: an important contribution to economic and social cohesion – Study.*

Gallo, C., Michele, G., Millard, J., Kåre, R., & Thaarup, V. (2014). *Study on eGovernment and the Reduction of Administrative Burden*. Luxembourg.

Gil-Garcia, J. R. (2012). *Enacting Electronic Government Success: An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions* (Vol. 31). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4614-2015-6

GSMA (2018). *Mobile Connect for Cross-Border Digital Services: Lessons Learned from the eIDAS Pilot.*

Guion, L. A. (2002). Triangulation: Establishing the Validity of Qualitative Studies.

Halmos, A. (2018). Cross-border digital public services, 55–66.

Hatzopoulos, V. (2008). Assessing the Services Directive (2006/123/EC). *Cambridge Yearbook of European Legal Studies*, *10*, 215–261. https://doi.org/10.1017/S1528887000001324

Hedström, K., Wihlborg, E., Gustafsson, M. S., & Söderström, F. (2015). Constructing identities – professional use of eID in public organisations. *Transforming Government: People, Process and Policy*, *9*(2), 143–158. https://doi.org/10.1108/TG-11-2013-0049

Hinsberg, H., Kala, K., Kask, L., & Kutt Anders (2020). *Study on Nordic-Baltic Trust Services.*

IDABC (2007). Data Interchange – IDABC. Retrieved from https://www.efta.int/~/media/Files/Publications/Fact%20sheets/EFTA%20participation%20in%20EU%20programmes/IDABC-Programme.pdf

The IDABC Programme (2005-2009).

Identity Documents Act (n.d.). Identity Documents Act – Riigi Teataja. Retrieved from https://www.riigiteataja.ee/en/eli/ee/526042018001/consolide/current

Kalvet, T., Toots, M., & Krimmer, R. (2018). Contributing to a digital single market for Europe. In *Janssen, Chun et al. (Ed.) 2018 – Proceedings of the 19th Annual* (pp. 1–8). https://doi.org/10.1145/3209281.3209344

Kamelia Stefanova, & Dorina Kabakchieva and Roumen Nikolov (2010). Design Principles of Identity Management Architecture Development for Cross-Border eGovernment Services, *8*(2), 189–202. Retrieved from www.ejeg.com

Klimkó, G., Kiss, P. J., & Kiss, J. K. (2018). The effect of the EIDAS Regulation on the model of Hungarian public administration. *Central and Eastern European EDem and EGov Days*, *331*, 103–113. https://doi.org/10.24989/ocg.v331.9

Kubicek, H. (2010). Introduction: conceptual framework and research design for a comparative analysis of national eID Management Systems in selected European countries. *Identity in the Information Society*, *3*(1), 5–26. https://doi.org/10.1007/s12394-010-0052-0

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. https://doi.org/10.1007/s12394-010-0063-x

Laurent, M., Denouël, J., Levallois-Barth, C., & Waelbroeck, P. (2015). Digital Identity. In *Digital Identity Management* (vol. 115, pp. 1–45). Elsevier. https://doi.org/10.1016/B978-1-78548-004-1.50001-8

Leitold Herbert, & Posch Reinhard (2012). Stork – Technical Approach and Privacy. In J. Bus (Ed.), *Digital enlightenment yearbook 2012* (Vol. 0, pp. 289–306). Washington, D.C: IOS Press. https://doi.org/10.3233/978-1-61499-057-4-289

Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy*, *10*(1), 8–25. https://doi.org/10.1108/TG-11-2013-0047

Leosk, N., Põder, I., Schmidt, C., Kalvet, T., & Krimmer, R. (2021). Drivers for and Barriers to the Cross-border Implementation of the Once-Only Principle. In R. Krimmer, A. Prentza, & S. Mamrot (Eds.), *Lecture Notes in Computer Science. The Once-Only Principle* (Vol. 12621, pp. 38–60). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-79851-2_3

Leyman, F. (2012). Electronic Governance and Cross-Boundary Collaboration // E-Government Implementation in Belgium and its Link with the European Dimension: Innovations and Advancing tools. In Y.-C. Chen & P.-Y. Chu (Eds.), *Electronic* *governance and cross-boundary collaboration: Innovations and advancing tools / Yu-Che Chen, Pin-Yu Chu, [editors]* (pp. 65–85). Hershey, Pa.: Information Science Reference. https://doi.org/10.4018/978-1-60960-753-1.CH004

Lips, M. (2008). *Identity Management in Information Age Government: Exploring concepts, definitions, approaches and solutions.*

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.), *Communications in Computer and Information Science. Electronic Governance and Open Society: Challenges in Eurasia* (Vol. 1349, pp. 75–89). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-67238-6_6

Lusoli, W., Maghiros, I., & Bacigalupo, M. (2008). eID policy in a turbulent environment: is there a need for a new regulatory framework? *Identity in the Information Society*, *1*(1), 173–187. https://doi.org/10.1007/s12394-009-0011-9

Mahula, S. (2020). *Opportunities and challenges for self-sovereign identity in the public sector: a case of Belgium* (Master Thesis). KU Leuven.

(2009). *Malmo Ministerial Declaration on eGovernment*. Retrieved from https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf

Mariën, I., & van Audenhove, L. (2010). The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society*, *3*(1), 27–41. https://doi.org/10.1007/s12394-010-0042-2

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, *3*(1), 213–233. https://doi.org/10.1007/s12394-010-0044-0

Melin, U., Axelsson, K., & Söderström, F. (2016a). Managing the development of e-ID in a public e-service context. *Transforming Government: People, Process and Policy*, *10*(1), 72–98. https://doi.org/10.1108/TG-11-2013-0046

Melin, U., Axelsson, K., & Söderström, F. (2016b). Managing the development of e-ID in a public e-service context. *Transforming Government: People, Process and Policy*, *10*(1), 72–98. https://doi.org/10.1108/TG-11-2013-0046

Procedure for formation and issuance of personal identification codes - Riigi Teataja (2021).

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ (Clinical Research Ed.)*, *339*, b2535. https://doi.org/10.1136/bmj.b2535

Monfort, V., Krempels, K.-H., Majchrzak, T. A., & Turk, Ž. (2016). *Web Information Systems and Technologies* (Vol. 246). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-30996-5

Myhr, T. (2008). Legal and organizational challenges and solutions for achieving a pan-European electronic ID solution. *Information Security Technical Report*, *13*(2), 76–82. https://doi.org/10.1016/j.istr.2008.06.001

Nielsen, M. M. (2017). *eGovernance and Online Service Delivery in Estonia*. Staten Island, NY, USA. https://doi.org/10.1145/3085228.3085284

OECD (2011a). *DIGITAL IDENTITY MANAGEMENT Enabling Innovation and Trust in the Internet Economy.*

OECD (2011b). *Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers* (No. 186). Paris. Retrieved from OECD Digital Economy Papers website: http://dx.doi.org/10.1787/5kg1zqsm3pns-en https://doi.org/10.1787/5kg1zqsm3pns-en

OECD (2020). *One-Stop Shops for Citizens and Business*. Paris. Retrieved from OECD Best Practice Principles for Regulatory Policy website: https://doi.org/10.1787/b0b0924e-en https://doi.org/10.1787/b0b0924e-en

Pedroli, M., O'Neill, G., Fravolini, A., & Marcon, L. (2021). *Overview of Member States' eID strategies*. Brussels. Retrieved from Delloite website: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/National+Strategies?preview=/364643428/364643437/eID_Strategies_v3.1%20(2).docx

Peristeras, V., Tarabanis, K., & Loutas, N. (2007). Cross - Border Public Services: Analysis and Modeling, 101. https://doi.org/10.1109/HICSS.2007.158

Pöhn, D., & Hommel, W. (2020). IMC: A Classification of Identity Management Approaches. In I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, . . . A. Sasse (Eds.), *Lecture Notes in Computer Science. Computer Security* (Vol. 12580, pp. 3–20). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3_1

Police and Border Guard Board Estonia (2019). *Estonian eID scheme: Technical specifications and procedures for assurance level high for electronic identification.*

RIA.ee (n.d.). Electronic Identity eID | Estonian Information System Authority. Retrieved from https://www.ria.ee/en/state-information-system/electronic-identity-eid.html

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. https://doi.org/10.1007/s10207-017-0385-x

Roelofs, F. (2019). *Analysis and comparison of identification and authentication systems under the eIDAS regulation* (Master Thesis). Radboud University.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5. ed.). Harlow: Financial Times Prentice Hall.

Schellong, A. (2004). *Extending the Technology Enactment Framework*. PNG Working paper No. PNG07-003.

Schweighofer, E., & Hötzendorfer, W. (2013). Electronic identities – public or private. *International Review of Law, Computers & Technology*, *27*(1-2), 230–239. https://doi.org/10.1080/13600869.2013.764142

Sealed, & time.lex and Siemens (2010). *Study on Cross-Border Interoperability of eSignatures (CROBIES)*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/crobies-study-cross-border-interoperability-esignatures-2010

Servida, A. (2019, July 3). *Let's go eIDAS: building trust online: Towards Trustworthy Digital Identities in Europe Brussels,*. Retrieved from https://digitalenlightenment.org/system/files/andrea_servida_eidas.pdf

Shehu, A., Pinto, A., & Correia, M. E. (2019). On the Interoperability of European National Identity Cards. In P. Novais, J. J. Jung, G. Villarrubia González, A. Fernández-Caballero, E. Navarro, P. González, . . . D. Durães (Eds.), *Advances in Intelligent Systems and Computing. Ambient Intelligence – Software and Applications –, 9th International Symposium on Ambient Intelligence* (Vol. 806, pp. 338–348). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-01746-0_40

Single Digital Gateway Regulation (2018).

SK solutions (n.d.). SK - About SK. Retrieved from https://www.skidsolutions.eu/en/about/

Sousa, L. de (2013). Understanding European Cross-border Cooperation: A Framework for Analysis. *Journal of European Integration*, *35*(6), 669–687. https://doi.org/10.1080/07036337.2012.711827

(2017). *Tallinn Declaration on eGovernment: at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017*. Retrieved from https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

Thales Group (n.d.). Electronic ID cards in Belgium: the keystone of eGovernment. Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/belgium

Turner, D. W., III (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators, *15*(3). Retrieved from https://nsuworks.nova.edu/tqr/vol15/iss3/19

(2020). *State of the Union Address by President von der Leyen at the European Parliament Plenary* [Press release]. Brussels. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

Veiga, L., Janowski, T., & Barbosa, L. S. (2016). Digital Government and Administrative Burden Reduction. In *Bertot, Estevez et al. (Ed.) 2016 – Proceedings of the 9th International* (pp. 323–326). https://doi.org/10.1145/2910019.2910107

Vries, H. de, Bekkers, V., & Tumers, L. (2016). INNOVATION IN THE PUBLIC SECTOR: A SYSTEMATIC REVIEW AND FUTURE RESEARCH AGENDA. *Public Administration*, *94*(1), 146–166. https://doi.org/10.1111/padm.12209

Walliman, N. (2011). *Research methods: The basics / Nicholas Walliman*. *The basics*. London, New York: Routledge.

Whakapapa Maori (n.d). Whakapapa Maori Structure, Terminology and Usage. Retrieved from https://maaori.com/whakapapa/whakpap2.htm#Introduction

Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, *23*(1), 17–35. https://doi.org/10.1057/ejis.2013.34

World Bank Group (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.*

Yin, R. K. (2018). *Case study research and applications: Design and methods* (Sixth edition). Los Angeles: SAGE.

Appendix

A Interview partners

Table 6 List and details of the interviewees

Interviewee	Organisation	Dates	Duration
Expert A	Estonian Information System Authority	8.6.2021	1 hour and 14 minutes
Expert B	Estonian Information System Authority	10.6.2021	40 minutes
Expert C	Estonian Information System Authority	10.6.2021	40 minutes
Expert D	Private Actor	2.6.2021	31 minutes
Expert E	BOSA IAA Department	11.6.2021	56 minutes
Expert F	ESSIF	9.6.2021	32 minutes
Expert G	Private sector / Digital identity	2.6.2021	28 minutes
Expert H	European Commission	11.6.2021	27 minutes
Expert I	Expert on digital identity	16.6.2021	27 minutes
Validation interviewee: Expert J	Expert on the cross-border eID and eIDAS	23.7.2021	59 minutes

B Interview guide

Thank you for participating in this interview. My name is Stefan Dedovic, and I am a final year student of the Erasmus Mundus programme in public sector innovation and e-governance. This interview is a part of my master thesis research dedicated to revealing the factors affecting the implementation of cross-border electronic identification from a national perspective.

It will be divided in two parts, one on the current implementation of cross-border eID and second about your opinion on the new proposal of the European Commission and European Digital Identity Wallet.

It will take around 35-45 minutes, and now I would like to ask your permission to record the conversation for my personal use, I will also anonymise the sensitive data.

The following blocks of questions were asked depending on the interviewee's profile, each aiming at uncovering different aspects of the RQ.

General Warm up Questions:

Could you describe me your experience and involvement in electronic identity management?

1. How is the electronic identity managed in your country?
    a. In your opinion, what are the main incentivising factors for notifying and implementing cross-border eID and your cases?

Technological questions

1. Could you please tell me to what extend implementation of cross-border eID affected the technological system of eIDMS in your country?
    a. What were the main challenges that you faced while implementing the cross-border eID?
    b. What were the main driving factors that affected the technological changes if they happened in your country?
    c. How did you overcome them?

2. Regarding the eIDAS nodes and implementation of them have you had any challenges or barriers to implement them? How did you overcome? What are the recommendations?

Organisational and institutional questions:

2. Could you please tell me to what extent the implementation of cross-border eID affected the your eIDMS from organisational point of view?
    a. What were the main challenges that your organisation faced in the cross-border eID implementation?
    b. What were the driving factors that influenced those changes, if happened?
    c. What factors had a negative impact on the implementation of the cross-border eID?
    d. How would you overcome these challenges and barriers?
3. To what extend did cross-border eID affected the cultural/legal/ institutional system in your country?
    a. Have you faced any challenges from institutional perspective and point of view with implementation of cross-border eID? Did it affected your provision of eIDs to citizens?
    b. In your opinion how would you overcome these barriers?

NEW REGULATION:

4. In your opinion, how will this new regulation affect current process of development in cross-border eID? What do you expect will be the main challenges of this new proposal?
5. What are the benefits of this new proposal?
6. How the trust between parties will be enabled with European Digital Wallet?

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "YOUR TITLE HERE" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Münster, 08 October 2021

Stefan Dedovic

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Dedovic
Given Name: Stefan
Student number: 509668
Course of Study: Public Sector Innovation and eGovernance
Address: Schlossplatz 2, 48149 Münster
Title of the thesis: Factors affecting cross-border eID enactment in the EU The case of Belgium and Estonia

What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose, the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exmatriculation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

Tartu, Estonia, 09.08.2021

Stefan Dedovic