TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Helen Raamat 121790IABMM

ESTONIAN DIGITAL PUBLIC SERVICE IMPROVEMENT ANALYSIS IN CROSS-BORDER USE CASES

Master's thesis

Supervisor:	Innar Liiv
	PhD
Co-Supervisor:	Silvia Lips
	MSc

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Helen Raamat 121790IABMM

EESTI AVALIKE E-TEENUSTE PARENDAMISE ANALÜÜS PIIRIÜLESTE KASUTUSJUHTUDE JAOKS

Magistritöö

Juhendaja: Innar Liiv
PhD
Kaasjuhendaja: Silvia Lips
MSc

Tallinn 2021

Author’s declaration of originality

Estonian digital public service improvement analysis in cross-border use cases

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

Author: Helen Raamat

10.05.2021

Abstract

The aim of this thesis is to identify the main legal and technical barriers connected to the identity management and service provision that prevent the cross-border use of Estonian digital public service procedures and provide a solution of changes that can fit in the current e-government strategy and state of play.

The scope of this study focuses on a cross-border scenario where an alien with an electronic identity from one of the European Union Member States, wants to access one of the Estonian digital public service procedures.

In order to map the currently existing obstacles and a state of play, a document analysis and semi-structured interviews were conducted with digital public service providers in Estonia. The analysis investigates how to resolve the cross-border interoperability issues that the digital public services are currently facing. This was achieved by exploring the existing state-of-play for cross-border use cases through a process design and highlighting the requirements for cross-border interoperability infrastructure.

As a result of the analysis, the author provides recommendations how the existing barriers that affect cross-border digital public service delivery in Estonia could be overcome by introducing the changes in a TO-BE process model.

Keywords: interoperability, cross-border digital public services, eIDAS, SDGR, implementation challenges, electronic identity.

This thesis is written in English and contains 79 pages, 6 chapters, 14 figures and 3 tables.

Annotatsioon

Käesoleva magistritöö eesmärk on uurida ja välja selgitada, millised on peamised eksisteerivad barjäärid, mis takistavad Eesti avalike e-teenuste piiriülest pakkumist nii õiguslikust, organisatoorsest, tehnilisest kui funktsionaalsest vaatest ning pakkuda välja lahendus koos potentsiaalsete muudatusettepanekutega, mis sobituksid Eestis juurutatud avalike e-teenuse pakkumise kontseptsiooni.

Magistritöö skoop käsitleb kasutusjuhtu, kus Euroopa Liidu riigi kodanik, kes kasutab oma koduriigi elektroonilist isikutuvastusvahendit, soovib kasutada Eesti avalikku e-teenust ja soovib saada juurdepääsu selle teenuse protseduuridele.

Selleks, et kaardistada hetkel eksisteerivad barjäärid ja hetkeolukord, viis töö autor läbi dokumendianalüüsi ja pool-struktureeritud intervjuud Eesti avalike e-teenuse pakkujatega. Analüüsi käigus uuris töö autor, kuidas leida parim lahendus Eesti avalikke e-teenuseid mõjutavatele piiriülese koosvõime probleemidele. Selleks kaardistas autor olemasoleva olukorra piiriüleste avalike e-teenuste pakkumisel läbi e-teenuste protsesside kirjelduste, tuues välja olulisemad nõuded piiriülese piiriülese koostalitlusvõime infrastruktuuri näitel. Analüüs põhineb kvalitatiivsel juhtumianalüüsil, kus analüüsiti kahte ühtse digivärava määruse lisas II toodud avaliku teenuse protseduuri.

Käesoleva magistritöö analüüsi tulemusena pakkus autor välja soovitused, kuidas leida lahendus olemasolevatele barjääridele, mis mõjutavad piiriüleste avalike e-teenuste pakkumist Eestis. Selleks koostas autor eelneva analüüsi ja juhtumisuuringute põhjal täiustatud protsessimudelid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 79 leheküljel, 6 peatükki, 14 joonist, 3 tabelit.

List of abbreviations and terms

CEF	*Connecting Europe Facility*
EC	*European Commission*
EESSI	*Electronic Exchange of Social Security Information*
EES	*Estonian e-government system*
eHDSI	*e-Health Digital Services Infrastructure*
EIF	*European Interoperability Framework*
eID	*Electronic Identification*
eIDAS	*The regulation on electronic identification and trust services for electronic transactions in the internal market*
RIA	*Information System Authority*
ERA	*Estonian Road Administration*
ESIB	*Estonian Social Insurance Board*
ETCB	*Estonian Tax and Customs Board*
EU	*European Union*
EUCARIS	*European car and driving license information system*
GDPR	*General Data Protection Regulation*
HWISC	*Health and Welfare Information Systems Centre*
IMI	*Internal Market Information System*
ISKE	*Three-level IT Baseline Security System*
MI	*Ministry of the Interior*
OOP	*Once-Only Principle*
PIC	*Personal Identification Code*
SCOOP4C	*Stakeholder Community Once-Only Principle for Citizens*
SDGR	*Single Digital Gateway regulation*
SPOCS	*Simple Procedures Online for Cross-border Services*
STORK	*Secure identity across borders linked*
TOOP	*The Once-Only Principle Project*
UML	*Unified Modeling Language*

Table of contents

List of figures

List of tables

1 Introduction

In the era of digital revolution, electronic identification (eID) and trust services are the essential components to enable secure transactions in the digital world. The mobility of European Union (EU) citizens has increasingly grown in the recent years, as well as the demand and expectations to the access to cross-border digital public services. In order to support the objectives of the digital single market and digital economy, the regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was established on July 23rd in 2014 in EU. The aim of the eIDAS is to facilitate the access to cross-border digital services by creating trust in the digital world alike in the physical world. According to the regulation, all the public and private sector authorities providing digital public services in EU must mutually recognize the notified eID means [1]under eIDAS. For the implementation of eIDAS, European Commission's (EC) Connecting Europe Facility (CEF) has created an eID building block that provides a framework and a software platform for cross-border interoperability – eIDAS-Node [11]. As of 2020, the majority of EU member states have already implemented eIDAS-Node in their national eID infrastructure. Although, the eIDAS-Node software platform enables to provide a functionality for cross-border identification in EU digital public services, the accessibility to the cross-border digital service procedures under eIDAS framework remains low.

The implementation of Single Digital Gateway Regulation (SDGR) foresees the increased use of electronic identification (eID) transactions across the EU. Therefore, it is necessary to specify what the cross-border eID infrastructure must provide in order to meet the needs and expectations for the Single Digital Gateway initiatives.

Most of Estonian digital public services require that the user has an existing record in the national registries or an existing Estonian national identifier in order to gain full access

[1] Notification of electronic identification schemes by Member States is a prerequisite of mutual recognition of electronic identification means [31].

to the digital public services and online procedures. Nevertheless, this is a much wider issue in EU than just the case of Estonia. On the other hand, Estonian eID means are notified under the eIDAS from November 2018 [10], i.e. they are enabled for use towards EU digital services, but there are only a small number of digital public services provided by other EU countries accessible for cross-border use today. Although, few countries within EU have already implemented their country specific identity verification systems for identity matching, there is no commonly agreed approach and guidelines how the cross-border data and evidence exchange for such use cases should be performed. As foreseen in the SDGR, work on resolving this interoperability issue is inevitable from the aspects of cross-border service provision. Although, the focus of this study has been set specifically on the Estonian perspective of digital service provision, the outcomes of this study could be adopted as an example by other countries that have similar e-government infrastructures.

1.1 Purpose of the study

The principle aim of this thesis is to identify the main legal and technical barriers connected to the identity management and service provision that prevent the cross-border use of Estonian digital public service procedures and provide a solution of changes that can fit in the e-government strategy and state of play.

During the research, various legislative and regulatory documents were analyzed, as well as previous researches and findings, to formulate a uniform understanding of the recent developments and solutions in cross-border services and identity management.

The scope of this study focuses on a cross-border scenario where an alien with an eID from one of the EU Member State wants to access one of the Estonian digital public service procedures. In order to map the current existing obstacles and a state of play, a document analysis and semi-structured interviews were conducted with digital public service providers in Estonia.

The analysis investigates how to resolve the interoperability issues that the digital public services are currently facing. This was achieved by exploring the existing state-of-play for cross-border use cases through a process design and highlighting the requirements for cross-border interoperability infrastructure. The analysis focuses on two online procedures of the SDGR's Annex II that will be treated as separate cases. As a result of the analysis, the author provides recommendations how the existing barriers that affect cross-border digital public service delivery in Estonia could be overcome.

1.2 Motivation of the study

The author of this thesis is a student of Business Information Technology study program in Tallinn University of Technology while also working in the area of e-government. As the mobility of the citizens in EU has increased significantly in the past years, the cross-border interoperability of eID and the demand of seamless access to digital services without the bureaucratic burden has become inevitable. The COVID-19 pandemic has urged to even faster uptake and development of digital public services and procedures to be performed online. Therefore, analyzing the improvement of cross-border service provision in Estonia also complies with the author's professional interest in this topic.

This study seeks to facilitate the provision of the cross-border digital services and procedures in Estonia and compliance with the legal frameworks in EU, focusing on the recent developments of eIDAS and SDGR. The main outcome of this research is to provide practical recommendations for the implementation of cross-border digital services in Estonia that could improve the overall service consumption experience for EU citizens. Considering the obstacles identified in the study and the enablers of EC's existing building blocks that support cross-border interoperability and service delivery, the service improvement analysis will be performed.

This study focuses specifically on the Estonian perspective of service provision however, the outcomes of this study could be adopted by other countries that have similar e-government infrastructure and processes. The author also hopes that the outcomes of the analysis will provide a valuable input to Estonian public administrations and public service providers, but, as well, to the EC to consider future improvements on revising the regulatory policies and existing cross-border interoperability services and platforms.

1.3 Research questions

This thesis seeks the answers to the two main research questions (RQ) which are divided into associated sub-questions (SQ).

In the first research question, the author seeks to identify which are the main barriers in cross-border digital public service provision and how these barriers affect a seamless public service delivery in Estonia on legal, organizational, technical and operational level. Based on the literature review, the previous studies have identified several barriers in the cross-border service provision in the EU, which will be further analyzed in this research on the case of Estonia. In order to find answers to the research questions, a qualitative data analysis will be conducted using multiple sources of information. In addition, the qualitative thematic analysis will be used to validate the findings from the document analysis.

RQ1. What are the key barriers that prevent seamless digital service delivery of Estonian public services in cross-border use cases by the means of EU member state notified eID?

- *SQ 1.1. How the barriers affect seamless delivery of Estonian digital public services in cross-border use cases on the legal, organizational, technical and operational level?*

The second research question focuses on the practical part of the research, by analyzing the qualitative data from the documentation and interviews, to understand the current state of play, the concepts and expectations of the cross-border service provision and how does the existing infrastructure support the cross-border digital public service delivery in Estonia. Based on the input obtained from the qualitative research data, the key requirements for a seamless cross-border service delivery in Estonia will be formulated. The proposal of changes with recommendations for future implementations will be presented based on two SDGR online procedures.

RQ2. How the cross-border infrastructure should to be improved for a seamless cross-border digital public service delivery in Estonia?

- *SQ 2.1. What are the key requirements for a successful implementation of a fully digital cross-border public service?*

1.4 Thesis outline

This thesis is divided into 6 chapters. The first and present chapter gives an overview of the purpose and motivation of the research, and provides an overview of the research questions. The second chapter conducts a literature overview of the related work. The third chapter of this thesis sets a theoretical foundation by focusing on the key factors influencing the cross-border service provision and concepts of interoperability in Estonia. The fourth chapter introduces the research design and methodological approach used in this thesis and explains the data collection procedures and analysis methods. In the fifth chapter, the author provides an overview of the research analysis and findings, discusses the results and provides recommendations. The sixth and final chapter of this thesis summarizes and presents conclusions of the research and provides future directions of the study.

2 Related work

In this chapter, the author will review the previously written literature to provide a high-level summary of what has already been done in the area connected to this research topic and to identify possible gaps in the field.

As the focus of this research is to analyze the possibilities of improvement of cross-border service provision in Estonia, it is important to be familiar with the legal conditions, but also from the technical and operational point of the aspects. The inclusion criteria for the previously written literature for this research was based on the purpose of this research and author's own experience on working with different interoperability frameworks and regulations.

Various researches have analyzed the legal and technical constraints in connection to different cross-border initiatives across EU. This literature review of related work will provide an overview of the overall impact of the main legal, organizational, technical and operational constraints and how they have affected the digital service provision in Estonia.

2.1 Compatibility of the eIDAS Regulation with the Estonian e-government system

The goal of adoption of the eIDAS in 23 July 2014 was to provide an EU-wide legal framework that enables secure and seamless electronic interactions between businesses, citizens and public authorities [11].

The recognition of EU electronic signatures became mandatory to all member states on July 2016 and the recognition of cross-border eID for electronic identification on September 2018 [5] [10]. In order to support the interoperability of eIDs, the European Commission (EC) created the eID and eSignature building blocks to help member states' public administrations and digital service providers to extend the existing infrastructure for a secure cross-border service delivery [13]. In order to create trust in cross-border transactions, the regulation has described the evaluation process of member state's national identification systems, which is the basis of mandatory recognition of eIDs across EU[5]. As of 2020, Estonia has implemented the EC eID and eSignature building blocks that enabled the use of cross-border electronic identification means and electronic signatures across the digital public services.

Gerli Aavik [7] has evaluated compatibility of the eIDAS with the Estonian e-government system (EES) by analyzing whether the changes introduced by eIDAS would be complementing or challenging for Estonian e-government national goals and initiatives, such as SignWise, e-residency and other bilateral agreements on cross-border eID interoperability. The author used the empirical analysis and Content, context and process (CCP) framework's dimensions for assessing the compatibility of the eIDAS with the EES. However, this study remained limited due to the fact that at the time of the study, the eIDAS had not been adopted its implementation acts yet. Therefore, the practical content of the eIDAS was discussed based on the speculations [7].

Before the eIDAS was introduced, there were several pan-European pilot projects initiated in the EU, such as the Secure identity across borders linked (STORK) and the Simple Procedures Online for Cross-border Services (SPOCS), that had successfully proved the necessity for the eIDAS framework that enables mutual cross-border recognition and interoperability of eIDs across the EU. The new regulation and framework have certainly created a number of enablers for cross-border digital interactions by establishing a uniform framework, however, it does not exactly refer to any classification of the mandatory digital public services that must be available for citizens and businesses. Over the years, Estonia has been continuously investing into building its e-government that has proved to be the biggest enabler for fast adoption of cross-border initiatives and one of the first enabler for cross-border digital service delivery [7]. By allowing transparent digital decision-making and paperless communication between government and citizens, Estonian e-government has considered to be internationally recognized as "the most advanced society in the world" [16].

According to the CCP analysis, most of the mismatches between the contents of EES and eIDAS were considered minor, but some mismatches were identified as more substantial in the CCP dimensions, such as technology, information and staffing and skills that require:

- revision of national regulations and policies (concerning the data privacy and validity measures);

- creating additional competencies in the state (at legal and technical level);
- financial investments for the adoption of eIDAS eID building blocks and for the technical implementation [7].

Although, Estonia has had other cross-border initiatives, apart from the eIDAS, the new regulation does not compete or limit the existing initiatives, but provides a uniform interoperability framework that can conform with all the EU member states. One example of an existing cross-border initiative that has been implemented in Estonia, before eIDAS was introduced, is the Estonian e-residency. Although, eIDAS could possibly decrease the EU market for e-residency in some aspects, the majority users of e-residency are considered to be from the non-EU countries. Moreover, the eIDAS cross-border interoperability between EU e-governments would increase the interest in the non-EU countries [7].

Aavik has highlighted one possible barrier regarding the digital identity that could affect the overall interoperability across EU. Considering the importance of secure identification and authentication means across EU digital services, the digital transactions using electronic identity should include unique identifiers. It has been identified that there are numerous of EU countries that are unable to provide numeric personal identifiers that are persistent in time due to historical, cultural or religious reasons. In Estonia, the uniqueness of a personal identifier is the fundamental element in the EES and the same principles are expected to be fulfilled from the EU digital identities, to enable eID interoperability [7]. However, the identifiers can vary across different electronic identification means in one country, which can lead to interoperability issues.

Since Estonia has been able to actively participate in the development process of eIDAS, the interests that are important from the EES perspective, are represented in the regulation. That involvement has been one of the most important factors that allows easy adoption of the eIDAS in the EES. The findings in Aavik's research show that, although the eIDAS is to serve the wider goals of the EU, there are no major changes foreseen in the existing building blocks of the EES, and the changes that are introduced with the eIDAS are rather complementing the goal and interests of EES and national initiatives. Apart from the compatibility aspect, it should be noted that every successful adoption of international-wide framework should include comprehensive communication at both, international and national level [7].

Following the previously highlighted gaps in the regulation, as of 2020, the EC has opened a public consultation to re-evaluate the eIDAS regulatory framework with a goal to gather feedback from the member states about the existing drivers and barriers that impact of the current implementation and uptake of digital identity and trust services in EU [11].

2.2 The impact of Single Digital Gateway Regulation

The aim of the Single Digital Gateway Regulation (SDGR) is to facilitate the digital access to cross-border administrative services for citizens and businesses by enabling the full potential of digital single market and eliminating administrative burdens. One of the main elements of the SDGR, the European single entry "Your Europe" portal, will provide the necessary guidance citizens and businesses need in order to have an easy access to European digital administrative services in compliance with the four freedoms of European single market - the free movement of goods, capital, services, and people. The regulation stands for the equality of the access to online procedures, which means that the procedures accessible for national citizens must be equally accessible across the borders. The second element of SDGR, set in Article 14, is the establishment of the technical solution of Once-Only principle (OOP) that enables cross-border evidence exchange in compliance with the data protection law and General Data Protection Regulation (GDPR). This allows citizens and businesses to provide the information to public administrations only once and will challenge the public administrations to implement a secure cross-border data exchange solution for the direct evidence exchange between authorities [18][19].

Since the SDGR is a newly developed framework, there are only few earlier studies that provide comprehensive analysis on the impact of SDGR. Rakshya Bhattarai [12] has analyzed the impact of SDGR in Estonia from the EU students' perspective. The study analyzed the overall application and public administrative processes that the EU students, who intend to start their studies in Estonia, must follow. The SDGR highly bases on the existing digital ICT infrastructures built in members states. Since Estonia has one of the most advanced e-government with interoperable systems in EU, the technical implementation of SDGR could be achieved with less effort than for the countries without a proper digital government infrastructure. The availability of digitalized public services is the integral part of implementing interoperable platform for cross-border digital transactions. The high number of digitalized public services in Estonia is definitely a big advantage on the fast implementation of the SDGR. However, the understanding of how the internal processes of digitalized public services are affected when adopting the regulation, is important [12].

The Article 4 of the SDGR has set the principles for the online accessibility of the information regarding public administrative procedures for citizens. Apart from the objectives of Your Europe portal, Estonia has already an existing national single-entry portal, the state portal of Estonia, that fulfills the requirements set in Article 4 [2][12].

According to the Article 6 of the SDGR, the EU states must ensure the fully digital cross-border access to the procedures listed in Annex II of the regulation for the users. In particular, the regulation requires that the procedures must be carried out fully digitally, without the physical presence of the person at any stage of the process. This means that the public administrations responsible for provision of those procedures must be ready to exchange the data and evidence with the corresponding authorities in the other member states. Although, a concession can be made in exceptional cases, where the public interest is affected in the areas of public security, public health or cases of fraud, but the member state must limit the physical presence, where possible. In any of such exceptional cases, the member state must provide a comprehensive description of the circumstances behind the exception. On the example of Estonian service delivery, there are currently several steps in public service procedures that require a physical presence. For example, the requirement of physical presence applies when a person from other EU country moves to Estonia on the basis of studying, working or other matters. Thereafter, registering a place of residence in population registry is required in order to get the Estonian personal identifier and thereby, have the possibility for digital access to government services and for issuing the Estonian ID card [2][12]. In such cases, the physical presence is clearly justified in support of the public security to avoid cases of fraud, but it can be argued, whether the security aspects can or cannot be fulfilled fully online.

The regulation also sets requirements in the Article 9, 10 and 11 for quality requirements related to information on rights, obligations and rules, procedures, assistance and problem-solving services. Based on the study on student application process, all the related procedures were identified to already meet the quality measures determined by the regulation [2][12].

According to the findings, the implementation of SDGR should not affect the vital part of the service delivery in Estonia, but the processes of the procedures might need to be somewhat adjusted to comply with the regulation [12]. However, the given conclusions in the research were limited to only one of the many processes and procedures listed in the regulation – studying abroad. In order to have a more precise overview of the overall impact to the EES as a whole on the implementation of SDGR, a further analysis involving different digital services and electronic procedures should be performed.

2.2.1 Once Only principle

The SDGR Article 14 sets requirements to establish a technical system for the cross-border automated data and evidence exchange between competent authorities in different member states and the application of the OOP for the online procedures listed in Annex II and to the procedures in directives 2005/36/EC[1], 2006/123/EC[2], 2014/24/EU[3] and 2014/25/EU[4] [2]. The aim of the Article 14 is to minimize the administrative burden for citizens and businesses. By the end of 2023, the citizens and businesses must be able to perform the procedures subject to the regulation in all EU member states without any physical presence. The public authorities are, therefore, entitled to exchange the data and evidence in an automated way, so the data that has been provided once, must be reusable in other procedures, while respecting the data protection regulations. In support to the contribution on enabling efficient Digital Single Market, the EC has initiated two projects in EU that have been working on the establishment of technical infrastructure that will enable OOP for the SDGR – the Once-Only Principle Project (TOOP) and the Stakeholder Community Once-Only Principle for Citizens (SCOOP4C). TOOP has been focusing on facilitating the exchange of business-related data and evidence to reduce the administrative burden for public authorities and businesses. SCOOP4C has put the effort on investigating how the OOP for citizens can be successfully implemented. There are

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0036

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0025

also a number of initiatives in Europe that are supporting the cross-border service provision, such as the eGovernment Action Plan 2016-2020[1] and the Tallinn Declaration on eGovernment[2] [17][20][21][22].

The requirements for the technical system of OOP in the SDGR are currently defined only at a basic level since the regulation has not adopted its implementing acts yet. TOOP is considered so far to be an existing proof-of-concept of the cross-border OOP architecture and, therefore, it is a good starting point for the creation of EU-wide OOP interoperability architecture and a technical system and thereby, will provide a valuable input to the creation process of the regulation’s implementing acts. TOOP has also initiated a recent collaboration with the Connecting Europe Facility (CEF), working together towards the architecture and implementation of the technical system foreseen in the SDGR Article 14 [17][23].

Various research papers have tried to map the barriers that might challenge the process of adopting cross-border OOP. The technology and interoperability are foreseen as one of the most challenging aspects on the implementation of cross-border OOP as the ICT systems in different countries can vary significantly. This, in turn, creates a numerous of barriers, such as incompliance with the OOP requirements, differences in the legacy systems, different approaches on the data management, etc. In the context of the legal and regulatory factors, the limitations to the OOP might apply when it comes to data and evidence sharing across the borders. Also, in the earlier studies, it has been argued, whether the uptake of OOP will significantly increase without the legal force. In order to reduce these obstacles, the EC has adopted the SDGR [24].

2.3 Cross-border e-Government Services in the Baltic Sea Region

The research article [25] introduces the study performed under the DIGINNO project that seeks to identify the major barriers towards the availability of cross-border digital government-to-business in the Baltic Sea region. The study identified the language and

[1] https://ec.europa.eu/digital-single-market/en/european-egovernment-action-plan-2016-2020

[2] https://ec.europa.eu/digital-single-market/en/news/ministerial-declaration-egovernment-tallinn-declaration

electronic identification and authentication as two of the most dominant obstacles among the Baltic Sea region in development of cross-border services for business [25].

The language barrier aspect will likely to be overcome with the adoption of SDGR and Your Europe portal. Since Estonia has established the quality measures regarding the accessibility to digital services and procedures, the language barrier problem does not affect the current implementation [25].

The national eIDs have been the central enabler in delivering digital public services to citizens and businesses. The second barrier that was identified in the study mainly concerns the EU countries that have not yet fully implemented the changes and requirements introduced by eIDAS. The SDGR and eIDAS together create a powerful enabler towards delivering e-services across the EU. A cross-border measures of the mutual recognition of electronic identities are already implemented in Estonia and are increasing [25].

Another barrier mentioned among the findings of the study, where the availability and validity of electronic documents was considered crucial, only appears to be important in several very specific use cases [25].

2.4 Research gap

According to the findings in previous studies, over the past decade the EU has introduced various regulations and acts that directly apply to the EU Member States that has had an impact, not only to the national legislation, but also to the concept of cross-border interoperability and service provision.

The literature review of related studies revealed several gaps in the field that could be investigated more closely:

- The compatibility analysis of the eIDAS with the EES was conducted while eIDAS implementing acts were not adopted yet. Therefore, the practical content of the eIDAS needs a further research;
- According to the findings of Bhattarai [12], the implementation of SDGR should not affect the vital part of the service delivery in Estonia, but the processes of the procedures might need to be somewhat adjusted to comply with the regulation

[12]. However, the given conclusions in the research were limited to only one of the many processes and procedures listed in the regulation – studying abroad. In order to have a more precise overview of the overall impact to the EES as a whole of the implementation of SDGR, further analysis involving different digital services and electronic procedures should be performed.

3 Theoretical framework

The focus of this study relies on the concepts of the cross-border interoperability of digital public services in EU as a theoretical framework.

The societies are moving fast towards a digital future by digitalizing procedures for businesses and governments. Digitalization in the public sector reduces administrative burden and promotes seamless and efficient communication with public administrations for citizens and businesses. On 2016 the Digital Single Market Strategy for Europe published the eGovernment Action Plan 2016-2020[1] accelerating the digital transformation of government. [33]. The goal of the new eGovernment Action Plan was to eliminate existing barriers through the digitalization of public administrations by setting up joint vision and principles for EU:

"By 2020, public administrations and public institutions in the European Union should be open, efficient and inclusive, providing borderless, personalized, user-friendly, end-to-end digital public services to all citizens and businesses in the EU. Innovative approaches are used to design and deliver better services in line with the needs and demands of citizens and businesses. Public administrations use the opportunities offered by the new digital environment to facilitate their interactions with stakeholders and with each other."[33].

The eGovernment Action Plan has introduced the following principles and priorities for the public service digitalization in EU:

- Digital by default
- Interoperability by default
- Cross-border by default
- Once-Only principle
- Inclusiveness and accessibility
- Openness & transparency
- Trustworthiness & Security [33].

[1] https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

As a reaffirmation of commitment on the vision and principles laid down in the eGovernment Action Plan, all the EU member states and EFTA countries agreed to sign the Tallinn Ministerial Declaration on eGovernment [35].

As by 2021, there have been remarkable improvements on the uptake of digital public services, where already 58% of citizens in the EU prefer communicating with public administration using digital channels and procedures. The recent developments in public sector digitalization has increased the overall online availability of digital public services in EU up to 82%. As a comparison, 99% of state provided services are already available online in Estonia [42]. Moving towards to more digitalized society will lead to even higher expectations in public administration’s performance [34]. In spite of the success we have reached with digitalization by today, the government digital transformation needs continuous effort and improvement [33].

3.1 Interoperability

3.1.1 Concept and principles

In the need of specific common guidance on creating interoperable and high-quality digital public services, on 23 March 2017 European Commission adopted the European Interoperability Framework (EIF). The framework covers 12 underlying principles of European public services:

1. Subsidiarity and proportionality
2. Openness
3. Transparency
4. Reusability
5. Technological neutrality and data portability
6. User-centricity
7. Inclusion and accessibility
8. Security and privacy
9. Multilingualism
10. Administrative simplification
11. Preservation of information

12. Assessment of Effectiveness and Efficiency

The EIF presents an interoperability model, where the interoperability is classified into four layers [32].

Legal interoperability. In each government, the legal frameworks, strategies and policies are different, which can make achieving to an interoperable level quite challenging. Legal interoperability foresees that an assessment of any impacts or barriers for technical design in legislation should be identified as earliest as possible to reduce the costs and time of the overall implementation of digital public services [32].

Organizational interoperability. The organizational layer of interoperability aims that the digital public service provision should rely on the commonly accepted business modelling standards and methods. Having an organizational interoperability in place ensures that the public service delivery is user centric and unambiguous [32].

Semantic interoperability. The underlying idea of semantic interoperability is to ensure that the exchanged data across governments and borders are following the same commonly established standards. The semantic interoperability can be improved, e.g. using data-driven-design principles along with data linkage technologies. Having semantic interoperability is a critical factor for a seamless data exchange and management. The lack of semantic interoperability can become a major threat for the overall interoperability achievement and result misfunctioning digital public services [32].

Technical interoperability. Achieving technical interoperability involves following the common standards of when designing a technical architecture and standards for public services. Technical interoperability is difficult to achieve across EU without common building blocks and standards. [32]. Fortunately, during the past decade, EC has been working on creating common technical solutions that support the technical interoperability [11].

3.1.2 Interoperability services

EC in collaboration with CEF Digital has created large variety of interoperability services, also commonly known as Building Blocks. These Building Blocks consist frameworks, set of standards and reference software. Since the development and provision of the Building Blocks are made under the supervision of EC, the compliance with the EU legislation can be ensured [13].

CEF eIDAS eID

eID is an important tool in the European cross-border infrastructure. Majority of the digital public services require secure access to the electronic transactions and procedures in order to avoid data flaws or frauds. The eIDAS regulation supports the secure mutual recognition of cross-border eIDs, which is backed with a respective framework and a technical system of eIDAS-Node [38]. The eIDAS-Node software is a reference implementation of the eIDAS eID Profile and allows EU citizens to prove their identity and authenticate themselves with their national eIDs when using digital public services in another Member State [36]. The goal of the eIDAS-Node solution is to provide to all Member States with EU-compliant reference platform that enables interoperability between different eID protocols and standards [39]. In order to establish the cross-border recognition using eIDAS-Node software, the Member State has to configure the software in its national infrastructure and implement an interface between the national eID ecosystem and eIDAS network. The eID means that are notified under eIDAS Regulation can be used across the Member States digital public services [49].

eIDAS-Node supports two main cross-border scenarios:

1) Requesting a cross-border authentication

2) Providing a cross-border authentication

The general process of the cross-border scenarios starts with a citizen's request to access an online service on another Member State. Thereafter, the citizen needs to prove his/her identity using authentication with his/her national eID means. The eIDAS-Node system recognizes the request and redirects the citizen for authentication to the identity provider of his/her home country. After the successful authentication of a citizen, he/she will be redirected back to the online service provider, with an access to the service [39].

The high-level scheme in Figure 1 explains how the interoperability in the eIDAS Network is approached using the eIDAS-Nodes. As see from the figure, the eIDAS-Node consists of three components:

- **eIDAS-Proxy-Service**: a component that provides authentication data
- **eIDAS-Connector**: a component that requests cross-border authentication
- **eIDAS-Middleware-Service**: a component that provides authentication data and is being provided by the sending Member State and operated by a receiving member State [39].

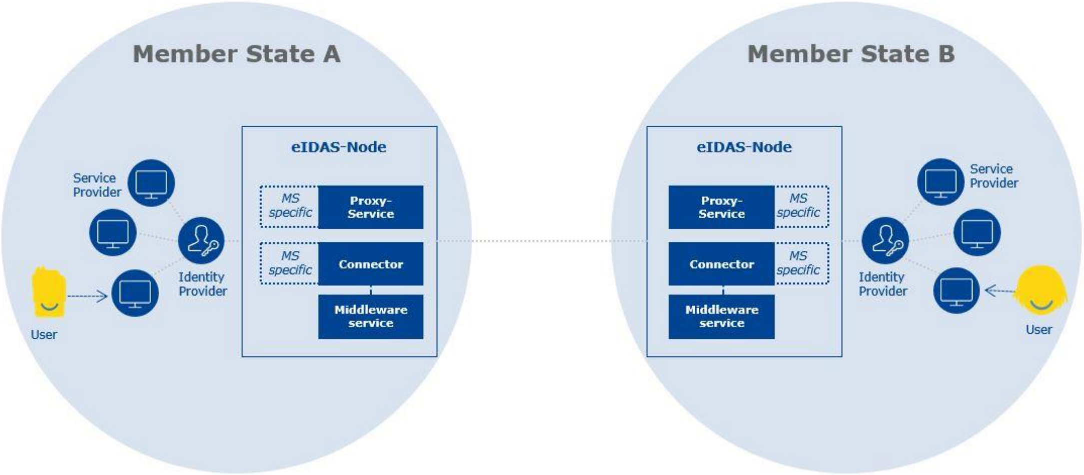

Figure 1. The overview of the interoperability components in eIDAS Network [39].

SDG Once Only Technical System

The Once Only Technical System is an EU-wide technical system currently under development supervised and provided by European Commission. The aim of the OOP system is to eliminate the administrative burden for citizens, public services and businesses in the EU and allow to share and reuse the data in real-time across borders. This will facilitate the access to public cross-border online procedures and provide an automated exchange of evidences [41].

As from technical perspective, the OOP system will be relying on open protocols and standards, the CEF and ISA building blocks and EIF. The architecture highly relies on the distributed architecture, where each Member State will be running the key elements of the system [41].

X-Road Data Exchange Layer

X-Road is an open-source software and a data exchange layer that enables a secure data exchange between information systems and is considered as the backbone of e-Estonia.

Currently, more than 1000 organizations and businesses in Estonia have become members of the X-Road ecosystem and are using it on a daily basis [43][45]. The following illustration in Figure 2 describes the X-Road ecosystem in Estonia.

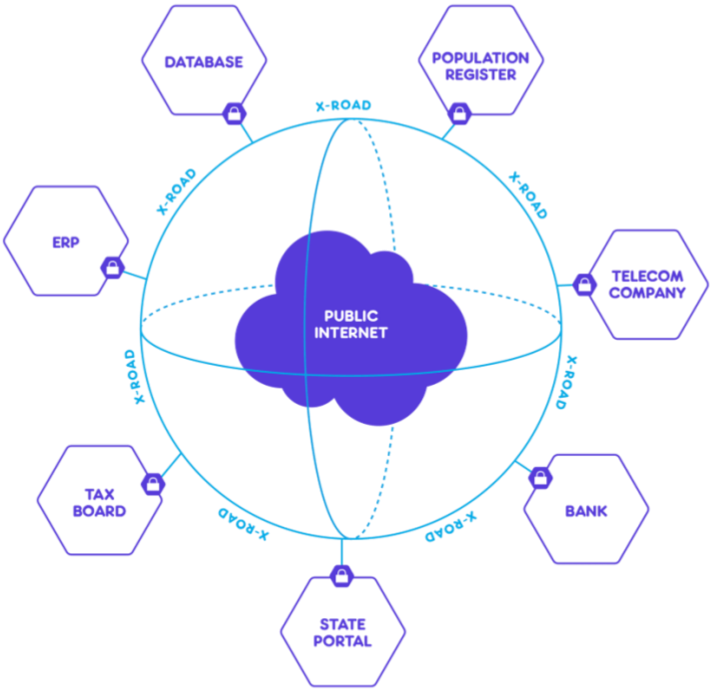

Figure 2. Estonian X-Road ecosystem [45].

X-Road also supports cross-border data exchange through federation, where the two X-Road ecosystems join together. The federation allows simple and secure cross-border data exchange between the ecosystems. As of today, Finland, Kyrgyzstan, Faroe Islands, Iceland, Japan and many other countries have already implemented their X-Road data exchange layer [43].

In order to assure data integrity, confidentiality and availability, the outgoing data is always being encrypted and signed and incoming data is being securely authenticated and logged [45].

Population Registry

The Estonian Population Registry, operated by the Ministry of the Interior, is the central database of identity attributes and other data related to a natural person residing in Estonia. The online service providers highly rely on the data available in the register [44].

The population register stores the following data about a natural person: given name and surname, birth data (date and place of birth), sex, personal identification code (PIC), citizenship, information on domicile and additional addresses, contact details (telephone number, e-mail address), information of the place of residence, marital status (single, married, widow/widower, divorced); information on mother, father, spouse and children, including right of custody; information on guardianship; restricted active legal capacity; data on death (the time and place of death); the highest completed education level and statement-based information about one's ethnicity, mother tongue and the highest completed education level [9]. The register also stores documents related to a natural person, such as personal identification document; marital status certificate; document which certifies the changing of one's data (concerning domicile and additional addresses, contact details, place of residence, the highest completed education level and statement-based information about one's ethnicity, mother tongue and the highest completed education level); the document changing Estonian citizenship; the document certifying the basis for legally staying in the country and the document certifying that a PIC has been issued; the individual's notices concerning their data; the notice of the issuer of the e-resident's digital identity document about the individual's e-residence. The use of information in the population register is regulated and guarded by Population Register Act[1] and the Personal Data Protection Act[2] [9].

The Population register has a vital role in issuing Estonian personal identification codes. PIC is a numeral combination of person's gender and a date of birth that allows unique identification of a person in Estonia. The underlying standard used in formation of PIC is EVS 585:2007 "Personal identification code. Structure", the Population Register Act and the procedure[3] for the formation and issue of a personal identification code. The Estonian PIC consists of 11 digits, where the first number refers to the gender and the following six numbers indicate the date of birth. The next three digits are sequential numbers issued for children born on the same day, and the last number is a "control number" that is being

[1] https://www.riigiteataja.ee/en/eli/502012019008/consolide

[2] https://www.riigiteataja.ee/en/eli/529012015008/consolide

[3] https://www.riigiteataja.ee/akt/108012019011

calculated according to a special formula. In Estonia, the PIC can be issued under the following conditions:

- after the birth to a child, the PIC will be created and added to the population registry along with the birth certificate by the health care institution or by the vital statistics department in Estonia;
- to a foreign citizen with no PIC, who has been part of a family event registered in Estonia (e.g. birth of a child or a marriage); in this case, the PIC will be issued by the vital statistics department in Estonia;
- to a person, who has been granted with a residence permit;
- to a person, who does not a permanent resident in Estonia, but need the PIC for the right to of entry his/her data in the database of Estonian public service providers [9].

The data interoperability between service providers and the register is achieved using X-Road system. This interconnection fulfills the principles of OOP and automated data exchange [44].

Estonian eID ecosystem

In Estonia, every person has the same exact identity in the digital and physical world. While there exist different eID carriers, the identity on these remain always the same. The eID in Estonia is operating on the basis of a Public Key Infrastructure model, having two different cryptographic keys: a public and private key. This model allows to perform secure transactions in the online services by authentication and digital signing [48].

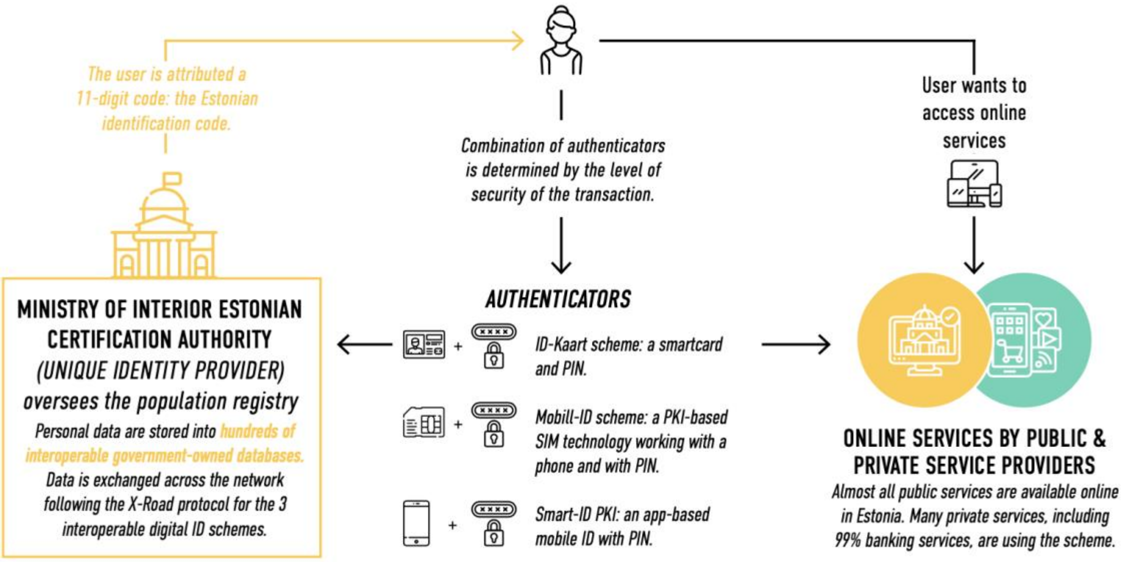
The user is attributed a 11-digit code: the Estonian identification code.
Combination of authenticators is determined by the level of security of the transaction.
User wants to access online services
MINISTRY OF INTERIOR ESTONIAN CERTIFICATION AUTHORITY
(UNIQUE IDENTITY PROVIDER)
oversees the population registry
Personal data are stored into hundreds of interoperable government-owned databases.
Data is exchanged across the network following the X-Road protocol for the 3 interoperable digital ID schemes.
AUTHENTICATORS
ID-Kaart scheme: a smartcard and PIN.
Mobill-ID scheme: a PKI-based SIM technology working with a phone and with PIN.
Smart-ID PKI: an app-based mobile ID with PIN.
ONLINE SERVICES BY PUBLIC & PRIVATE SERVICE PROVIDERS
Almost all public services are available online in Estonia. Many private services, including 99% banking services, are using the scheme.

Figure 3. Estonian eID ecosystem [42].

Authentication Gateway service

Information System Authority (RIA) operates an eID interoperability platform service, providing authentication with nationally and EU-recognized eID means for Estonian public service providers and citizens. The national eID means include ID-card, Mobiil-ID and Smart-ID authentication methods. The cross-border authentication with Member States' recognized eID means in TARA is enabled via eIDAS-Node reference software. This authentication platform (also known as "TARA") is by design eIDAS-compliant and widely in use in the public sector digital services in Estonia. The goal of having a centrally managed authentication service in Estonia is to provide a uniform user experience and reduce the administrative costs [46][47].

4 Research design and methodological approach

In order to analyze the cross-border availability of Estonian digital public service procedures in the context of the SDGR, to understand the obstacles in cross-border service provision and the requirements behind it, the qualitative research approach was adopted along with case study methodology as the leading methodology for this thesis.

Qualitative research methodology is an appropriate method to adopt in a research, where the topic requires more explorative approach and detailed understanding about the context of a problem. This can be accomplished by direct interaction with people, where the participants of the research can collaborate during the phases of data analysis and interpretation [26].

As the topic and research problem of this thesis focuses on the contemporary phenomenon to be explored in a real-life context, using multiple sources of evidence, qualitative case study research methodology was given priority [26]. Creswell [26] has successfully described case study as a research methodology and describes it as follows:

"Case study research is a qualitative approach in which the investigator explores a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information (e.g., observations, interviews, audiovisual material, and documents and reports), and reports a case description and case themes."

Yin and various other methodologists suggest that the most suitable research questions for designing a case study are to be formed starting with "how" and "why". However, the nature of the research questions in this study can successfully contribute in a case study design by mainly looking for answers to questions of "what", fostering the exploratory nature in the case study research [27].

During this research, the evidence was collected using multiple sources and different data collection methods, including documents, archival records and interviews. For the analysis, several qualitative data analysis techniques were used.

The overall research process used in this study is described in Figure 4.

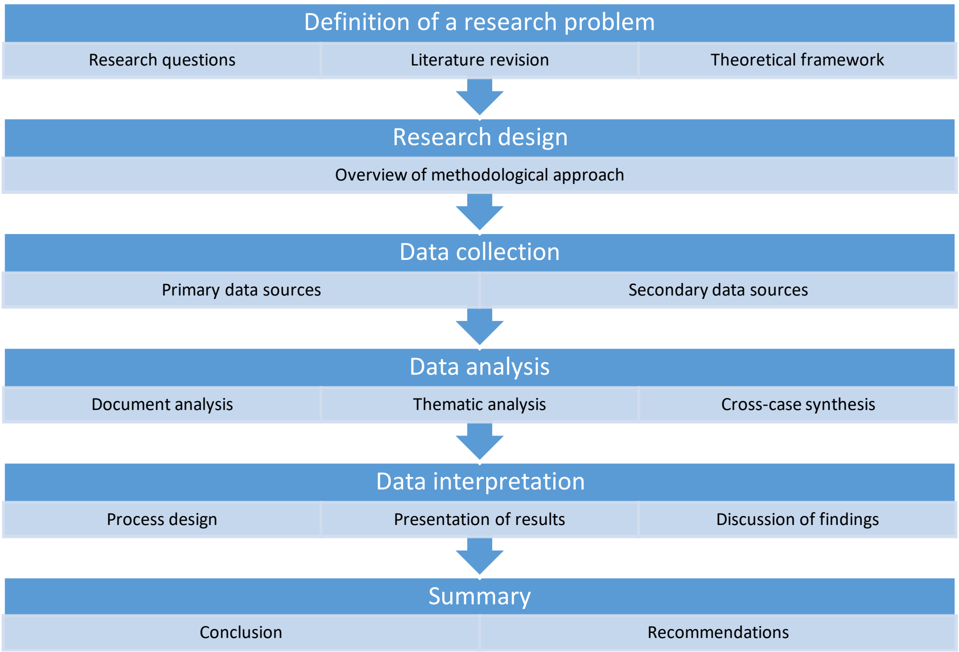

Figure 4. The overall research process.

To understand the impact of the requirements on the implementation of cross-border digital services in compliance with SDGR and strengthen the existing theoretical knowledge, it is important to provide a detailed overview of the processes that are affected. This was achieved through a descriptive case study, by mapping the current state of play of the cross-border service provision in Estonia and then providing an improved process design based on the SDGR online procedures. In order to improve the validity of the outcomes in this study, the author will analyze the two observed cases using cross-case synthesis method.

The ideas for the proposed solution were based on the input from the qualitative data analysis, as well as based on the author's own experience in the field of cross-border services and electronic identification. The results were validated through the identified requirements, process design and theoretical framework.

4.1 Data collection procedures

As specific for a case study, the data collection in this research involves multiple sources of information, including documentation and empirical data. Using multiple sources of evidence in a case study allows an in-depth analysis of the phenomenon and context of the study [27]. As driven from the research methodology and research questions, the author has built the analysis on both, primary and secondary sources of data.

4.1.1 Secondary data sources

For data collection from the secondary sources, various academic writings, formal studies, scientific reports, articles and technical documentation were used.

Documentation can provide a valuable input when conducting a case study analysis. The strengths of including documentation from different sources to the study allows the researcher to gather details to corroborate information from other sources and make inferences. However, it is important to keep the focus on the most pertinent information and to avoid being deviated by the abundance of documentation related to the research topic. It is also important to keep in mind that the inferences should be used rather as clues that need to be investigated further other than definitive findings [27].

4.1.2 Primary data sources

For data collection from the primary sources, semi-structured expert interviews were conducted during March and April in 2020 with the key stakeholders of the online electronic procedures specified in the Annex II of the SDGR.

The selection of interview participants was derived from the scope of the study and research questions. Single Digital Gateway Regulation outlines 21 services for cross-border delivery. As this research is focused on the online procedures defined in the SDG regulation Annex II, the author associated the aforementioned procedures with the corresponding public sector bodies. In order to achieve it, the author investigated each Estonian digital public service's that are directly linked with the SDGR Annex II procedures 21 procedures to associate with the corresponding service providers. As a result, 12 different public sector bodies were identified.

Upon the empirical data collection phase, 24 experts from 14 Estonian public sector bodies were contacted by e-mail and phone. In total, 14 interviewees responded with an interest to contribute or forwarded the request to the relevant experts and 10 interviewees did not respond. The target group of the interviews were conducted with IT managers, software architects and analysts, service managers and policy advisors. During the data collection phase, six expert interviews were conducted in total with various experts: four individual interviews and two group interviews. Four interviews were conducted during face-to-face meetings and two interviewees preferred to participate on the interview using Skype. The two group interviews were conducted, one with seven and the other with two interviewees. Using the mixed interview techniques in combination was not initially planned for a data collection for this research, but were developed based on the proposals from the interviewees, as it is important to create a comfortable atmosphere for the interviewee for a successful and fruitful interview. Furthermore, the group interviews and are considered to be rich in data and high on its quality [3]. Although, group interviews are typically structured in its form, the author chose to keep the semi-structured format throughout all the interviews as majority of the interviews were conducted in a semi-structured form.

Meuser and Nagel [3] discuss the expert interview as a specific form of applying semi-structured interviews, where the interviewees are of less interest as a (whole) person than their capacities as experts for a certain field of activity. They are integrated into the study not as a single case but as representing a group [3]. Semi-structured interview method was chosen for the data collection of this study as it gives a great flexibility to gain information in a less formal manner and, as well, to understand in more detail the interviewee's experiences. The interview questions were drafted and categorized prior to the interviews in order to keep the focus on topics that are important from the research perspective, but not strictly limiting it directly to the interview questions. As foreseen in semi-structured interviews, all interviews were covered with the same topics. Open-ended questions were presented at the beginning of each thematic topic and then the author moved to more specific questions. Some additional questions were addressed to clarify some aspects of the data that the interviewees had shared during the interviews in order to make correct interpretations of the data. At the end of each interview, the interviewees were free to address any other topics they wished to add to the previous discussion. The interview questions are presented in Appendix 1. The interviews were carried out in Estonian and were recorded using voice recording applications, Voice Memos by Apple and Skype call recording tool, for transcript writing and further analysis. An overview of participants is presented in Table 1.

When considering, whether the dataset collected was sufficient for this study, they author's' consideration was based on the scope of this research – the SDGR 21 procedures. During the data collection, 13 procedures out of 21 were covered with the 6 interviews. Nonetheless, the majority of procedures under the life events listed in SDGR's Annex II were covered, which included life events, such as birth, residence, working, moving, retiring and starting, running and closing a business (submitting a corporate tax declaration).

Table 1. List and details of the interviewees.

Government body	**Interviewee**	**Duration**
Ministry of the Interior	2 Experts from the Population Facts Department	53:43
Estonian Social Insurance Board	Expert from the Benefits Department	49:56
Estonian Road Administration	7 Experts from the E-services and Information Technology Department	55:11
Health and Welfare Information Systems Centre	Systems architect	51:29
Estonian Tax and Customs Board	Expert from the Tax Department	38:05
Estonian Tax and Customs Board	Expert from the Public Services Department	31:26

4.2 Data analysis procedures

In qualitative research, the analysis is often carried out in parallel with data collection. As the analysis can reveal the need for additional data sources, the parallel approach can become a useful method [37].

The data analysis in this research relies on three qualitative analysis techniques that were used to identify patterns, themes and sequences of the data that had been previously collected. Documenting at each step in the research analysis allows to achieve to trustworthy and valid conclusions that explains the chain of evidence to the readers [37].

4.2.1 Document analysis

After the data collection from secondary sources, a document analysis was used to build a comprehensive background of the phenomena, to identify the existing challenges and, thereby, adjusting the focus for this research. During the document analysis, multiple sources of documentation were used. The observations of case-relevant documents were made to highlight the findings and inferences found during the analysis. The pattern-matching logic was used to highlight the findings in document analysis.

In addition to the document analysis, qualitative thematic analysis was carried out to validate the findings with the Estonian digital service providers based on the use cases of SDGR during the interviews.

4.2.2 Thematic analysis

When seeking an appropriate qualitative data analysis method for the empirical data collected in this research, the qualitative thematic analysis was adopted. The interviews seeked, firstly, to understand the current concepts and business cases in cross-border service provision in order to analyze the AS-IS situation. Secondly, the interviews were used to investigate the business needs and requirements for the TO-BE cross-border service provision concept.

According to Braun and Clarke [1], there are six phases of thematic analysis, described as guidelines which will be followed in this research. It is important to recognize that qualitative analysis guidelines are exactly that – they are not rules, and, following the basic precepts, will need to be applied flexibility to fit the research questions and data. Furthermore, analysis is not a linear process where you simply move from one phase to the next and it is more of a recursive process, where you move back and forth throughout the phases [1].

According to the Braun and Clarke's guidelines [1], the first phase stands for getting familiar with the collected data, where active reading is crucial in order to get familiar with all the aspects of the data. In this phase, the verbal data, such as semi-structured interviews, will be transcribed into a written form in order to conduct the thematic analysis. During the transcription, the first ideas for coding will be drafted. The transcripts will be repeatedly checked against the interview recordings for accuracy of the data [1].

Once the author becomes familiar with the data and created an initial list of the first ideas, the production of initial codes from the data takes form. The process of coding is part of the analysis, as the data will be organized into meaningful groups. The transcriptions will be analyzed and initial codes will be identified based on the particular features of the data set, which are relevant to the research questions. Coding can be done either manually or using a software program [1]. As hand coding can be time-consuming process, even for a small number of interviews, a widely used qualitative software program, MAXqda, was used for the data analysis. Qualitative software programs are helpful tools for researchers, allowing to store and locate qualitative data in an efficient way. It facilitates assigning the data into a large set of codes and mapping the relationships between them. These are only few examples of qualitative software programs' features that makes the decision over hand coding a reasonable choice [15].

When all the data have been initially coded and collated, it is time to move to the phase three. This phase is where the interpretative analysis of the data occurs. The author proceeds with the comparison of the context behind the codes, analyzing the meaningful differences, similarities and the relations across the codes. The focus in this phase is on a broader level of themes, where the initial codes are being sorted to potential themes in relation to the research questions. For better visual understanding about the relationships between different codes and themes, the initial thematic map is introduced [1].

Phase four starts once the potential themes have been identified. During this phase, the previously identified themes will be reviewed and refined, including re-evaluating the thematic map. In order to do so, the potential themes will be, first, reviewed based on the collated data extracts to make sure whether they appear to form a coherent pattern and secondly, evaluated, whether the themes in the potential thematic map „work" in relation to the entire data set [1].

Phase five foresees further refinement of the themes that will be presented as part of the analysis. It is important to identify the essence of each theme, to understand what aspect of the data they capture and how the themes work together as an overall story in relation with the research questions [1].

The final phase in thematic analysis involves producing a report of the findings of the analysis. The author will present a story within and across the themes with a discussion in relation to the research questions [1].

4.2.3 Validity procedures

Data triangulation is considered an important approach within a case study research in order to increase the validity of a research. Triangulation involves multiple sources of evidence or approaches of analyzing the data, which can provide better and comprehensive understanding of the phenomenon. The purpose of the data triangulation procedure in this research is to provide multiple contexts to strengthen and enrich the understanding of the research questions [37][27][40].

4.2.4 Cross-case synthesis

In order to provide more practical and technology-oriented insight to this research, the author conducted a descriptive case study, based on two online procedures from SDGR Annex II.

The challenge in conducting a cross-case synthesis is the researcher's ability to develop strong, plausible and fair arguments that are supported by the research data [27].

As a result, the author proposes a solution how to improve the existing cross-border service provision process based on the theoretical framework and existing processes. The research results and TO-BE model will be evaluated towards the requirements arisen during the analysis and the theoretical framework. The UML diagrams used in this thesis are used to interpret, assess and validate he research results.

5 Research analysis and findings

To understand the impact of the requirements on the implementation of cross-border digital services in compliance with SDGR and strengthen the existing theoretical knowledge, a detailed overview of the processes will be provided using a descriptive case study method. This will be achieved by mapping the current state of play (AS-IS) of the cross-border service provision in Estonia and based on a cross-case synthesis, introducing improved processes (TO-BE) based on two of the SDGR online procedures.

In order to find answers to the first research question and its sub-questions, the qualitative data was collected from multiple sources and analyzed using pattern matching and themes.

To find answers to the second research question and its sub-questions, a cross-case synthesis along with the redesign of processes was conducted. The UML modelling techniques in this thesis are used to interpret, assess and validate he research results.

The ideas for the proposed solution were based on the input from the qualitative data analysis, but as well, based on the author's own experience in the field of cross-border services and electronic identification.

5.1 Document analysis

Cross-border service provision challenges

The implementation challenges of eIDAS and how to overcome these issues has become recently an important topic among the member states of EU, bringing together experts all across the EU to find a common approach [30].

According to the statistics of the Estonian state central authentication service (Figure 5), as of October 2020, the cross-border usage rate of Estonian digital public services with EU eID means constituted only 0,005 % of all monthly authentications [27].

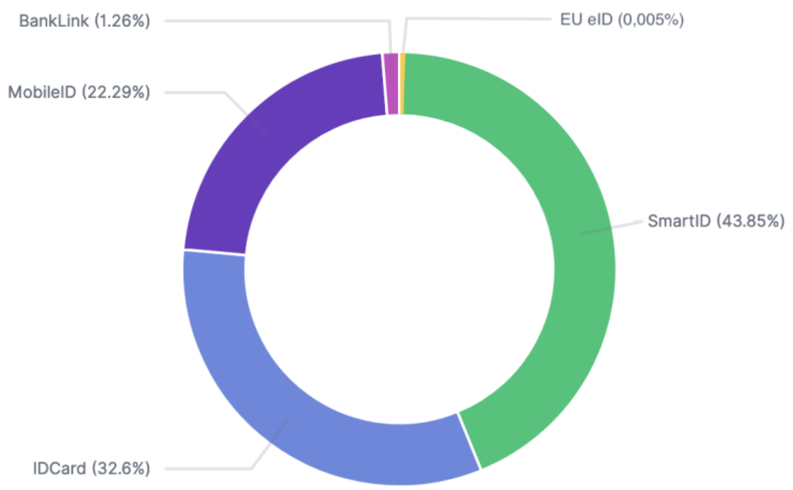

Figure 5. Monthly eID transactions in Estonian digital public services as of October 2020 [27].

On the other hand, the authentication requests issued with Estonian eID to use digital services in EU countries remained significantly higher, based on the statistics of Estonian eIDAS-Node system. The study on trust services in the Nordic-Baltic region also identified that the usage rate of cross-border digital services remains generally quite low [29].

In the following sections, the author will highlight the most significant factors that prevent seamless access to digital public services and online procedures in the EU.

Lips, Bharosa and Draheim [30] compared the challenges on implementing eIDAS between Estonia and Netherlands, where they have identified common challenges from various perspectives: compliance issues, interpretation problems, different implementation practices, collaboration, and the representation of legal person. The research reveals that previously identified challenges are likely to create additional barriers on collaboration between EU member states, citizens and service providers because of the insufficiency of common guidelines and standards, which cause different interpretations and practices that, in turn, can lead to system usability issues. The majority of the challenges are seen to be related to cross-border service provision [30]. In order to overcome those challenges, the study provided a set of proposals:

- analyze the possibilities to implement the common EU identifier
- specify the scope of a legal person in the regulation
- regulate the use of powers and mandates in the context of eIDAS
- develop a standardized testing framework for member states

- create common standards for unique identifiers
- provide recommendations for identity linking
- creating assessment guidelines for auditors
- develop a framework of standards for cross-border services
- publish and communicate usability guidelines for implementing cross-border services
- develop a central monitoring service to prevent security and availability issues [30].

Legal interoperability

The cross-border recognition of eIDs became mandatory on September 29th 2018, when the first eID scheme became notified under the terms of eIDAS. Estonia notified six national public sector-provided eID means, including ID-card, residence permit card, digital identity card, e-residency, digital identity card, mobile-ID and diplomatic identity card. As of today, already 15 Member States have notified their eIDs, where 14 of them are mandatory to recognize across the EU [10]. However, the complexity of the eID notification process slows down the recognition, and thereby the accessibility to the digital services and procedures for EU citizens. This could be considered as a potential obstacle for the cross-border interoperability [30].

From the policy aspect, one of the most crucial implementation barriers is that there is no EU-wide identifier that would provide a unique and persistent identifier on the access to digital services. Another important barrier in achieving common implementation guidelines appears to be driven from the differences between national legislations across the EU member states, which affects the cross-border service provision and access to online procedures. The interpretation of eIDAS itself is generally challenging, because of the lack of details in the context of definitions that leave too much room for interpretation and too little clarity and a weak link with associated regulations [30].

The lack of a common legal basis has prevented Member States from recognition of eIDs of other Member States. Therefore, the insufficient cross-border interoperability of national eIDs prevent citizens and businesses to access the digital public services in the EU [38].

Technical interoperability

From the service providers perspective, the most crucial challenges were identified to be a lack of guidelines for a cross-border incident management, missing self-compliance testing tools and framework, as well as the lack of guidelines and standards for unique identifiers of a natural person [30].

The mutual recognition of eIDs under the eIDAS Regulation aims to provide an access to the digital public services across the EU. The implementation of eIDAS is enabled by CEF Digital eID Building Block using eIDAS-Node software [49]. From a technical perspective, the trust establishment model is seen currently as an obstacle between the interconnection of eIDAS-Nodes, where the trust involves manual configuration of certificates and metadata. Any misconfiguration affects the availability of public online services and procedures. The Eurosmart study pointed out, as one of the potential solutions, to be establishing an automated trust mechanism where the trust and certificates can be managed centrally [49].

In the Article 13.2(c), the SDGR requires that cross-border users must be able to identify and authenticate themselves electronically in all the cases where it is possible for local users [2]. The OOP technical system foresees eIDAS as the appropriate solution for remote identification and authentication for SDGR online procedures. Deloitte study reports in its findings that several Member States require copies of ID documents to verify the identities of a person or to obtain additional data (e.g. nationality and citizenship) about a person that cannot be provided with the current eIDAS minimum data set [52].

Identity matching

Eurosmart has mapped the current state of play of the eIDAS implementation in EU and mapped as one of the obstacles to seamless cross-border recognition of eIDs to be identity matching. The study revealed that identity matching is one of the key issues from the national perspective. In many EU countries there is either no persistent identifiers or those identifiers are not part of the mandatory attributes [49]. The Annex of eIDAS Implementing Regulation on the interoperability framework has defined the minimum data set that EU Member States are obliged to provide for natural persons. The minimum data set includes the following attributes:

- current family name(s);
- current first name(s);

- date of birth;
- unique identifier [6].

According to the regulation, the unique identifier, constructed by the sending Member State, has to be follow the technical specifications of eIDAS eID profile [36] for cross-border authentication and be persistent in time [6]. The technical specifications specify the unique identifier in the following format, where:

- the first part of the identifier attribute is the code of the country that the identifier originates using one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/ ");
- the second part of the identifier attribute is the code of the country or international organization requesting a cross-border authentication using one of the ISO 3166-1 alpha-2 codes, followed by a slash ("/ ");
- the third part a combination of readable characters that uniquely identifies the identity asserted in the country of origin, but does not always reveal visible correspondence with the persons actual identifier (for example, username, fiscal number etc.) [50].

The additional data set for a natural person may contain the following additional attributes:

- first name(s) and family name(s) at birth;
- place of birth;
- current address;
- gender [6].

The Eurosmart study underlines that current legislation does not support the reliable matching of identities between the physical and digital identity referring that the technical specifications should set clearer requirements on natural persons identifiers. The limited number of mandatory attributes in the eIDAS regulation was considered as another obstacle to the cross-border service provision [49]. The identity matching systems allow to integrate multiple identities and link the cross-border identity to the existing records in the national registries [52].

If the public services that the citizens wish to access cannot match their identity to a record in the national systems, the access to the service may be declined, limitations to the procedures available online might apply or the paper-based solutions will be used as a fallback option. In case of the latter, a citizen would not be recognized according to the previously matched records [51].

When it comes to identity matching, the challenge arises on how to reduce false-positive matches. Artificial intelligence techniques and machine-learning algorithms might help out and provide more automated approach for identity resolution [51].

Member States of the EU have recently started to address more and more to this obstacle and are working towards finding a possible solution by exchanging practices on identity matching via eIDAS [51].

Communication

The Eurosmart study also pointed out that communication has often become an important barrier to a seamless implementation of eIDAS [49]. The main challenges from the user perspective are related to the accessibility and user experience when using cross-border services, due to the lack of well-communicated guidelines. Currently, the user journeys in digital services vary from country to country, while the user expects to follow similar journeys across services [30].

5.2 Thematic analysis

The thematic analysis was used to analyze the empirical data and highlight the themes identified during the analysis. As a result, the four themes were highlighted: 1) Accessibility, 2) Data exchange, 3) Identity management, 4) Interoperability. The selection of themes was based on the research questions. These themes highlight the key findings of the current state of cross-border service provision based on the SDGR services in Estonia and the main obstacles and requirements for a successful cross-border service delivery. The themes and codes are represented in the Figure 6.

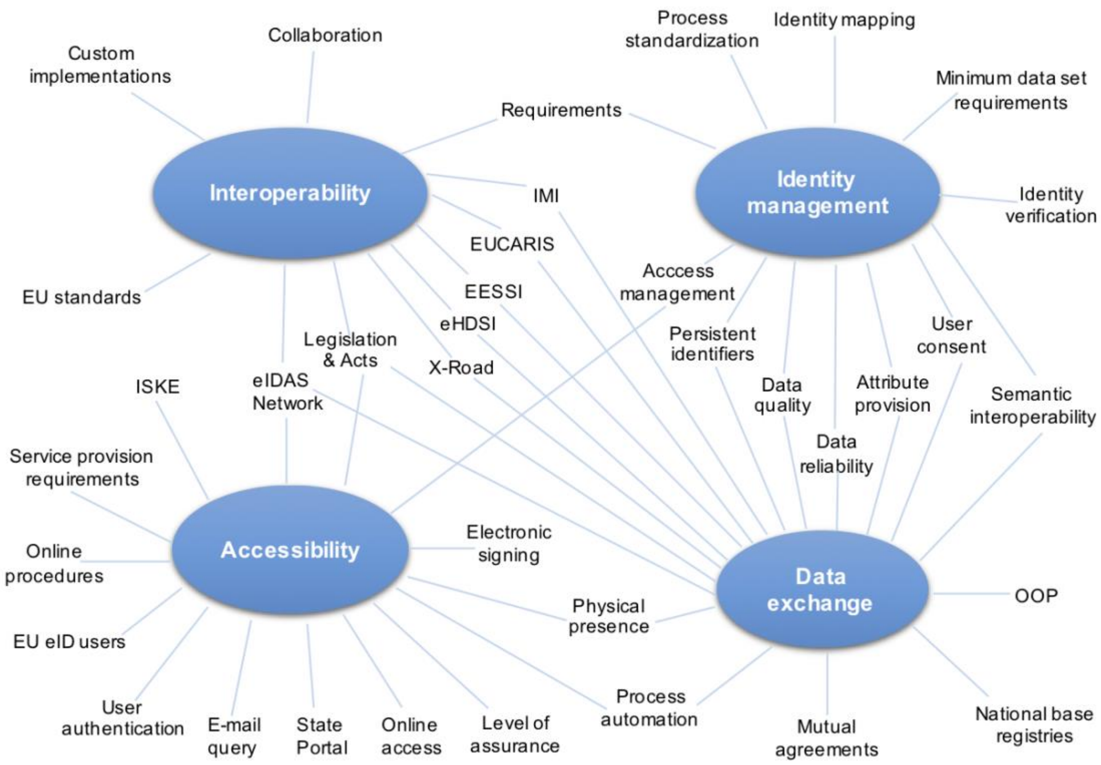

Figure 6. Thematic map.

Accessibility

Accessibility is, beyond a doubt, the most fundamental aspect when it comes to evaluation of the cross-border service provision. More than half of the interviewees pointed out that, even though there are fully automatized online procedures available for their public digital services today, they are not SDGR compliant yet. According to the interviewees, 9 out of 13 SDGR procedures that were addressed in the interviews are currently not accessible for EU eID users. More specifically, the interviewees said that six procedures concerning the scope of SDGR are currently under development and will be accessible as a fully online procedure in future. It was mentioned that most of the SDGR procedures are online and accessible via Estonian State Portal eesti.ee that provides digital access to the procedures to government services. One group of interviewees pointed out that not all the SDGR procedures are provided fully online, as required by the regulation, e.g. the procedure of registering a motor vehicle originating from or already registered in a Member State requires physical presence for both, national and EU citizens.

Regarding the access to the online procedures, the interviewees were asked which assurance levels of the eID means are required from EU eID users during authentication in their systems. All the interviewees hereby referred to the assurance level “high” according to eIDAS [5], since the Estonian government issued eID means (ID-card and Mobile-ID) are notified with assurance level “high”. Another popular approach of evaluating the assurance level was based on ISKE (three-level IT baseline security system) evaluation model, where the level of assurance defined in eIDAS Regulation is equalized according to the security class assigned to the information system. However, there was pointed out one SDGR procedure that does not require user authentication at any point of the process.

In order to obtain a better understanding about the complexity measure of the accessibility aspect in cross-border service provision, the interviewees were additionally asked, whether any of the procedures in SDGR Annex II requires digital signing at some stage of the process, but all the interviewees confirmed that there is no signing needed at any stage. An overview of the accessibility based on the SDGR online procedures is provided in the Table 2.

According to the interviewees, one of the most highlighted requirements by the current service provision concept was the presence of Estonian PIC. Without the latter, there are only few digital public services available for the EU eID users. The interviewees pointed out that the reasons behind the Estonian PIC requirement rely on the fact that the data about the authenticated user is requested from and being verified against the base registries, such as Estonian population register, using X-Road data exchange platform. Since the identity mapping highly relies on the existing records of a person in the base registries, the verification of EU eID users cannot be reliably performed without cross-border automated data exchange.

Table 2. An overview of the accessibility of SDGR online procedures

Procedures listed in Annex II of SDGR	**Accessible online**	**Requires user authentication**	**Requires signing**	**Physical presence required**
Requesting proof of registration of birth	Yes	Yes	No	Yes
Requesting proof of residence	Yes	No	No	No
Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004	Yes	Yes	No	No

Notifying changes in the personal or professional circumstances of the person receiving social security benefits, relevant for such benefits	Yes	Yes	No	Yes
Application for a European Health Insurance Card (EHIC)	Yes	Yes	Yes	No
Submitting an income tax declaration	Yes	Yes	No	Yes
Registering a change of address	Yes	Yes	No	No
Registering a motor vehicle originating from or already registered in a Member State, in standard procedures	N/A	N/A	Yes	Yes
Obtaining stickers for the use of the national road infrastructure: time-based charges (vignette), distance-based charges (toll), issued by a public body or institution	Yes	Yes	No	No
Obtaining emission stickers issued by a public body or institution	Yes	No	No	No
Claiming pension and pre-retirement benefits from compulsory schemes	Yes	No	Yes	No
Requesting information on the data related to pension from compulsory schemes	Yes	Yes	No	No
Submitting a corporate tax declaration	Yes	Yes	No	No

Data exchange

According to the interviewees' descriptions and the SDGR, one of the central enablers for cross-border service delivery is data exchange. The interviewees were asked to talk about the current data exchange model, involving the SDGR online procedures listed in Annex II. All of the respondents related to the usage of the X-Road as the backbone of Estonian e-government. The X-Road data exchange is based on the bilateral agreements between the service providers and registries. According to the interviewees, there are procedures that involve the data exchange between more than 25 different registries and databases which in terms of cross-border interoperability can be considered challenging. Several SDGR Annex II procedures that require cross-border data exchange are already covered with EU regulations, such as request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004.

It was highlighted by all the interviewees that one of the first and primary sources for the current identity mapping procedures rely on the data requested from the Estonian population register. The key requirement here is that there must be an existing record in the population register to perform a secure identity mapping procedure. For example, in order to request a proof of registration of birth, there must be a registered birth in the population register or in order to request a proof of residence, there must be already registered address in the register. Since there is no common standardized identity mapping procedure currently in use for the base registries, the data exchange of a new incoming EU eID user is blocked over the X-Road, which directs us back to the accessibility issue.

The two main common expectations that all interviewees addressed regarding the cross-border automatized data exchange in the context of SDGR, was the use of X-Road platform and persistent identifiers of the eID users.

Identity management

The identity management became the main talking point throughout the interviews that revealed some of the key obstacles in the current service provision concept. The interviewees were asked to describe how the identity mapping has been arranged in their systems today for EU eID users. It was pointed out by one interviewee that the population register has not yet analyzed how the EU identities can be verified. Therefore, there is currently no existing standardized and automatized identity mapping procedure that could resolve the availability issue for the online procedures at this moment. One of the most common cases identified by the interviewees, when the identity mapping becomes necessary, was when the EU citizen logs into a system for the first time, using EU eID means, and later applies for an Estonian eID. This creates a situation where multiple virtual accounts with different identifiers per one real identity in the databases and registries have to coexist. According to the interviewees, there are currently only manual procedures in use for identity mapping, that are not semantically interoperable across databases and registries. Three interviewees pointed out that they are generating temporary identifiers in the registries for the foreign nationals, e.g. upon the registration of a motor vehicle. It was highlighted that this has caused semantic inconsistencies between the national registries when it comes to the automatic data exchange, as is. Another identity and access management practice, that was pointed out by two interviewees, is creating a personalized account for foreign identities. For example, the foreign nationals, who are non-residents of Estonia nor have issued the Estonian PIC, will have to register themselves as a taxpayer in the register of taxable persons, where the proof of identity is required. After the verification of an identity by the officials, the account will be personalized and, thereupon, will have a granted access to the online procedures. One of the interviewees said that in the e-health sector the International Standardization Organization Object Identifier (ISO OID) standard has been adopted for describing the attributes, including the PIC, which creates a semantic systematization of different attributes across the e-health systems. In the Estonian e-health sector, there are specific OIDs described for each country, that will be applied as a prefix to foreign PICs. However, this solely does not resolve the identity mapping issue for foreign identities since there is no identity verification component in use.

As the discussion developed during the interviews, the interviewees were asked specifying questions regarding the requirements of identity mapping for an EU eID user. Across all the interviewees, the minimum data set requirements for mapping the identities of a natural person were pointed out as follows: first name(s), family name(s), PIC and date of birth. Some interviewees pointed out that they would require additional attributes, such as current address, country, gender, nationality and the place of birth. It was highlighted during the discussion that in many EU countries the current address is one of the most widely used additional attributes that are required in identity mapping processes, but since not many countries are providing this attribute in cross-border scenarios, it is quite difficult to perform the identity mapping. Thus, the efficient and reliable identity mapping should highly rely on the additional attributes that are persistent as possible in time.

Regarding to the attribute provision, all interviewees referred that the first queries about a natural person are always made to the Estonian population register and to the Estonian business register about a legal person. In addition, all the interviewees stated that the PIC is the key attribute that links the data in the registries across all the government online services to a natural person. Generally, the first query about a natural person is to validate, whether the PIC provided at the login exists at the population register. For example, when transferring the ownership of a motor vehicle to another person, the first owner only has to fill in the new owner's PIC and then the system makes an automatic query using the X-Road data exchange layer to the population register in order to fetch the person's data linked to that PIC. After the X-Road query to the population register, the requested data associated with the PIC will automatically appear in the system. This will prevent typological mistakes that might occur when the data is being filled in by the user and will, therefore, raise the accuracy of the data. However, this procedure is only applicable, when the person, who is a subject to identity mapping, has an existing record in the register.

According to the interviewees, the central issue that they are hoping to resolve in future, is to automatize the identity mapping procedures. Moreover, it was pointed out that in order to automatize the process, there should be internationally agreed standards how to semantically describe the identities across registries. Therefore, the semantic interoperability could bring the identity mapping to a next level. Also, it was pointed out that the PICs that are the subject for cross-border transactions, should include the country prefix since some EU countries may have identical structure of PICs, e.g. between Latvia and Estonia. However, this can be resolved by using eIDAS Network eID building block for EU nationals. Nevertheless, all the interviewees pointed out that the identities should be compared with the records in the Estonian population register. For some procedures, the population register currently stores the PICs of foreign nationals, but there are currently no identity mapping procedures in use.

Interoperability

In order to understand how the existing cross-border interoperability solutions support the cross-border service provision in overall terms, the interviewees were asked to describe their current infrastructure that supports cross-border transactions. According to the interviewees, there are several trans-European solutions based on EU legislation and interoperability agreements between European Union member states. Some of those examples, that have been implemented in Estonia and were highlighted by the interviewees, involve EESSI (Electronic Exchange of Social Security Information), eHDSI (e-Health Digital Services Infrastructure), EUCARIS (European car and driving license information system), IMI (Internal Market Information System) and eIDAS-Node. Among of all the aforementioned trans-European solutions, only eHDSI and eIDAS-Node are capable to perform automated data exchange. While EESSI, IMI and EUCARIS are used to exchange the information between government authorities only, the eHDSI and eIDAS-Node solutions are focused on the service provision from the citizen's perspective. It was pointed out that, apart from the EU digital services infrastructure, a widely used data exchange layer, X-Road, has been recently developed to the neighboring countries and is foreseen to have a lot of potential for cross-border data exchange in the future. Currently, there is an ongoing project that will establish the X-Road data exchange between Estonia and Finland for being able to mutually share and monitor the data in the registries. The interviewees explained that before the X-Road took international measures, there was a custom data exchange solution implemented in the region that involves data exchange between Finland and Estonia, Latvia and Estonia and Lithuania and Estonia. However, this solution is not fully automatized – the data from, e.g. Finnish register, is imported within a file once a week and is being manually imported into the Estonian population register, in order to obtain updated information about Estonians who are residing in Finland.

In order to understand the efficiency of the EU building blocks already implemented in Estonia, the interviewees were invited to describe how these interoperability solutions are currently supporting their business needs for cross-border service provision. According to the interviewees, the currently used EU building blocks for data exchange, such as IMI and EESSI are operational and cover the necessary business cases, but since they are based on non-automatized queries, getting the responses and, therefore, the overall procedure can be time consuming for beneficiaries. It was also pointed out by more than half of the interviewees, that currently there are not many SDGR Annex II online procedures available in Estonia for EU eID users who do not have an existing event in the population register nor have issued an Estonian PIC. The main cross-border automated data exchange obstacle, that was mentioned throughout the interviews, was that many countries do not provide a joint identifier for natural persons like in Estonia. For example, in Germany, each government authority assigns different identifiers to their citizens. That, in turn, brings along the mapping procedure. In case the latter could be automatized, the cross-border data exchange could raise the data quality significantly. One of the interviewees pointed out that there was an initiative between EU member states to create a common persistent identifier for taxpayers across the EU, but several countries did not support this initiative due to the legal constraints in their constitutional law. Since the countries were unable to agree in providing a common persistent identifier within EU, they are still standing in front of the initial issue with mapping multiple identifiers. Since the X-Road has been widely adopted in Estonia, the interviewees pointed out that using the same platform for cross-border transactions would be ideally the next step towards to an automatized data exchange between EU countries. The interviewees also pointed out that they would like to see more countries participating in the EU building blocks implementation.

The requirements for cross-border digital service provision improvement were composed, based on the interviewees responses that were highlighted through thematic analysis. The author created a list of high-level requirements, which are presented in Table 3. The key requirements will be, in turn, validated through a case study and a process design.

Table 3. Key requirements for cross-border digital service provision in Estonia.

ID	Requirement	Description	Theme
R-1	**Existing Estonian PIC**	One of the most highlighted requirements by the current service provision concept is having the Estonian PIC. Without the latter, there are only few digital public services available for the EU eID users. The data of authenticated user is requested from and being verified against the base registries, such as Estonian population register, using the X-Road data exchange platform.	Accessibility; Interoperability

R-2	**Existing event in the base registries (population register) for identity verification**	One of the first and primary sources for the current identity mapping procedures rely on the data requested from the Estonian population register.	Accessibility;
			Data exchange;
			Identity management;
			Interoperability

R-3	**Unified cross-border platform for automated cross-border data exchange**	Since the X-Road, which already permits the automated exchange of evidence, has been widely adopted in e-Estonia, using this platform for automated cross-border data exchange between EU countries would be preferred by Estonian digital service providers.	Data exchange; Interoperability

		The key requirement is that there must be an existing record in the population register to perform a secure identity mapping procedure. Since there is no common standardized identity mapping procedure currently in use for the base registries, the data exchange of a new incoming EU eID user's attributes is blocked over the X-Road, which directs us back to the accessibility issue.	
R-4	**Persistent PIC across EU**	Many countries do not provide a joint identifier for natural persons like in Estonia. For example, in Germany, each government authority assigns different identifiers to their citizens. That, in turn, brings along the mapping procedure. In case the latter could be automatized, the cross-border data exchange could raise the data quality significantly.	Data exchange Identity management Interoperability
R-5	**Automatized identity mapping procedure**	Since the identity mapping highly relies on the existing records of a person in the base registries, the online verification of EU eID users cannot be reliably performed without cross-border automated data exchange. The central issue that the service providers are hoping to resolve in future is to automatize the identity mapping procedures.	Identity management
R-6	**Standardized identity mapping procedure**	One of the first and primary sources for the current identity mapping procedures rely on the data requested from the Estonian population register. In order to automatize the process, there should be internationally agreed standards how to semantically describe the identities across registries. Therefore, the semantic interoperability could bring the identity mapping to a next level.	Identity management
R-7	**Sufficient provision of attributes for identity mapping**	The efficient and reliable identity mapping should highly rely on the additional attributes that are sufficient and persistent as possible in time, including: PIC, first name(s), family name(s), date of birth, country (as a prefix), current address, gender, nationality, place of birth.	Identity management
R-8	**Semantically interoperable attributes**	Semantically interoperable attributes are one of the key enablers for a seamless data exchange and data management.	Identity management

The documentation and thematic analysis identified a common issue of the current cross-border service provision concept across all the life events of the SDGR analyzed in this study – a lack of common understanding and non-existent standards for the identity management. The latter appeared to be the most crucial issue to the interoperability of EU digital public services.

5.3 Cross-case synthesis

In order to find answers to the second research question *RQ2. "How the cross-border infrastructure should to be improved for a seamless cross-border digital public service delivery in Estonia?"* the formulation of the requirements along with descriptive case study method will be conducted.

In this research, the author analyzed two case studies to validate the identified requirements. The author used descriptive case study research method to map the current state of play (AS-IS) that based on two online procedures of the SDGR's Annex II. The case inclusion criteria based on the use case definitions of SDGR online procedures from the study conducted by Deloitte [52], where the cases with lower level of cross-border evidence exchange were selected:

1) Requesting proof of residence

2) Requesting proof of registration of birth.

These two online procedures will be described during the cross-case synthesis and TO-BE processes will be used to highlight the possibilities and areas for improvement.

5.3.1 Requesting proof of residence: AS-IS

This procedure has only been identified in the Member States who have an established a national population registry. The procedure involves providing an extract of the registry to the citizen, where no additional evidences or documents need to be exchanged cross-border [52].

The registration of residence is necessary for the state and local government agencies to offer public services to people residing on their territory and to facilitate cooperation and information exchange. The submission of a notice of residence must be submitted when the individual changes the residential address in Estonia, moves to another country or from another country to Estonia [8]. Since the access to the Estonian population register's online procedures is permitted only with the national eID means (ID-card, Mobile-ID and Smart-ID), the EU citizens, who wishes to settle in Estonia or obtain the right of residence, must submit the notice of residence at the city or rural municipality government via an officer of population register by making a physical appointment. In case, the EU citizen is not the owner of the property, that is a subject to the notice, a document certifying the right of use of the property or a permission from the owner of the property to enter the property as a resident, must be submitted. Thereafter, the local government will verify within 10 working days of receiving a notice of residence, whether the notice complies with the requirements. In case the requirements were met, the residential address will be entered into the population register. However, there is an opportunity to submit the application electronically, by sending a digitally signed PDF document of the application and the consent from the owner with an email [8]. Upon the registration of residence. The EU citizens are automatically granted with a temporary residence permit of five years in Estonia. In order to be granted an ID-card, the EU citizen must turn to the Police and Border Guard Board after registering his or her residence [8]. The process of registering a place of residence is described in Figure 7.

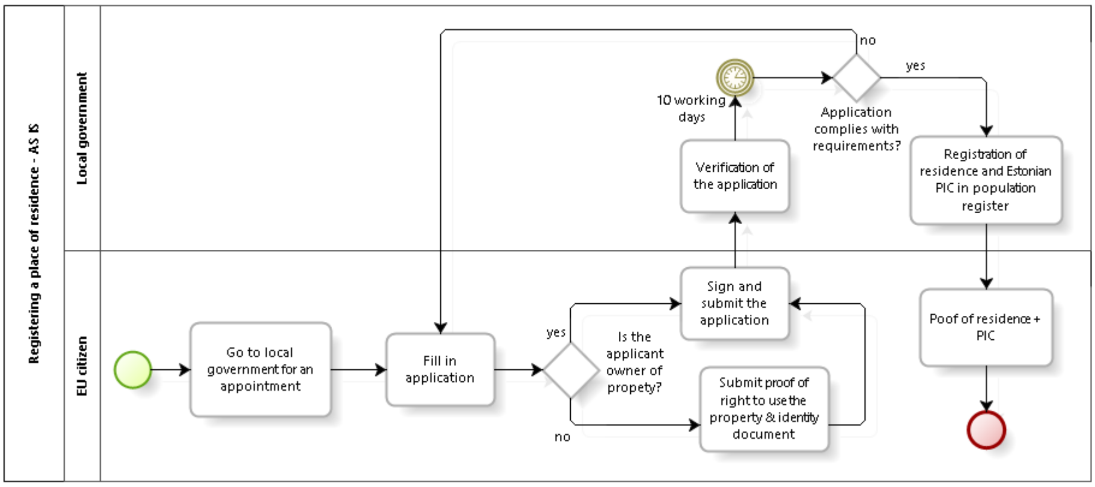
Registering a place of residence - AS IS
Local government
EU citizen
Go to local government for an appointment
Fill in application
yes
Is the applicant owner of propety?
no
Sign and submit the application
Submit proof of right to use the property & identity document
Verification of the application
10 working days
Application complies with requirements?
no
yes
Registration of residence and Estonian PIC in population register
Poof of residence + PIC

Figure 7. Process of registering a place of residence for EU citizen.

As highlighted during the analysis, most of the government digital services require Estonian PIC. According to the population register's procedures, the EU citizens can issue

Estonian PIC together with the notice of residence. For the latter, it is required to submit the application in person to the city or rural municipal agency of the residence.

The complete data requirements for the procedure of requesting a proof of residence are the following:

- First name(s) at birth;
- Family name(s) at birth;
- PIC
- Date of birth
- Place of birth
- Citizenship
- Nationality
- Native language
- Gender
- Address (including: country, state, parish/city, town, village, postcode, street, house/flat number)
- E-mail (only, when using online procedure) [8].

The following UML diagram in Figure 8 illustrates the steps that are required from EU citizen when requesting a proof of residence in Estonia, according to the standard procedures. Due to the lack of standardization on identity mapping procedures of EU eID users, automatic attributes exchange between the national registries using X-Road is not available.

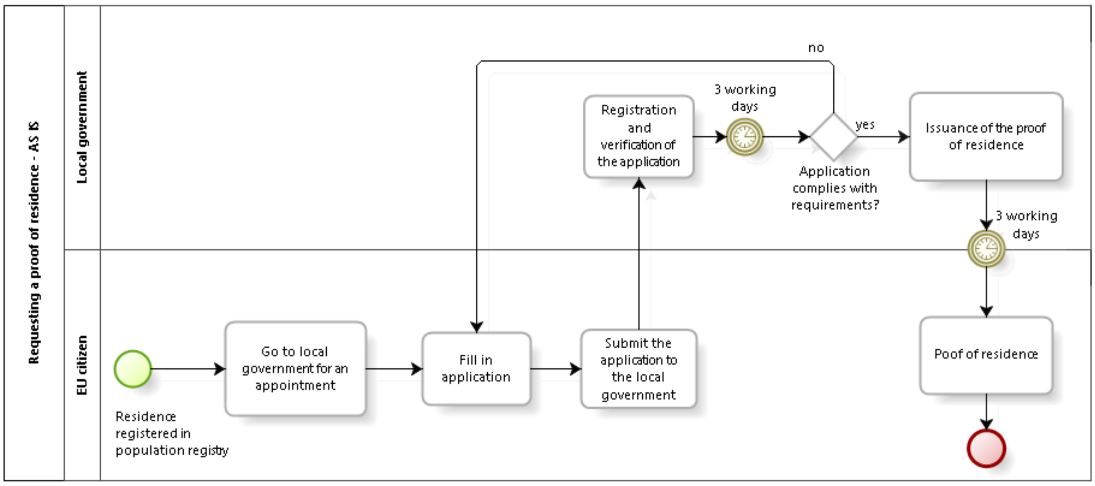
Requesting a proof of residence - AS IS
Local government
EU citizen
no
Registration and verification of the application
3 working days
yes
Application complies with requirements?
Issuance of the proof of residence
3 working days
Residence registered in population registry
Go to local government for an appointment
Fill in application
Submit the application to the local government
Poof of residence

Figure 8. Requesting a proof of residence – overall AS-IS process.

After the registration of residence and issuing the Estonian PIC, the EU eID user has fulfilled the requirement R-1 and R-2. After that, the EU citizen is permitted to apply for a residence permit card that can be used as an Estonian eID across digital services. In order to apply for it, the EU citizen must make another physical appointment. Since the digital public service providers must recognize the EU eID means notified to the European Commission (EC), the user can, therefore, sign in with and eID from his/her country of origin. The latter brings in the need for identity mapping. As the thematic analysis exposed, the identity mapping procedure should rely on the data stored at the Estonian population register as other registries make X-Road queries to validate the existence of the identity logged into their system. Due to the lack of standardization on identity mapping procedures of EU eID users, automatic attributes exchange between the national registries using X-Road is currently not available. As another remark, the online procedure for requesting proof of residence is currently only available at the State Portal webpage as an electronic PDF form to be submitted by email. The automated digital service for Estonian citizens to access this procedure should become available in the recent years.

5.3.2 Requesting proof of registration of birth: AS-IS

The second use case examined the life event in the SDGR Annex II, that covers an online procedure of requesting a proof of registration of birth. This procedure involves obtaining an extract from the national population register (or equivalent), where the cross-border exchange of additional information or evidences are not necessarily required to need to complete the procedure [52].

The birth is registered when the child is born in Estonia, one of the parents was born in Estonia or both of the parents are Estonian citizens. For example, upon the registration of the birth of a child, an entry of a child will appear in the population register with information about first and family names, gender, PIC, date and place of birth, parents' right of custody, residence and citizenship [9].

Since the eIDAS eID authentication is currently not available at the digital service of e-population register and the current service provision is available only offline, the physical presence of the EU citizen is the only option to access the procedure. In order for EU citizen to request a proof of registration of birth, an application can be submitted to any local government by a legal representative of the child [53]. The complete data requirements for the procedure of requesting proof of registration of birth are the following:

- First name(s) at birth;
- Family name(s) at birth;
- PIC
- Citizenship
- Date of birth
- Gender
- Data of identity document (including: country, type, number, date of issue)
- Address of residence (including: country, county, municipality/town, village/street, building, flat)
- Contact details (including: phone number, email address, postal address)
- Marital status
- Nationality
- Native language [53].

Similar data set applies when requesting other types of certificates, such as: marriage certificate, death certificate, divorce certificate and change of name certificate [53]. The following UML diagram in Figure 9 describes the steps that are required from EU citizen when requesting a proof of registration of birth in Estonia, according to the standard procedures.

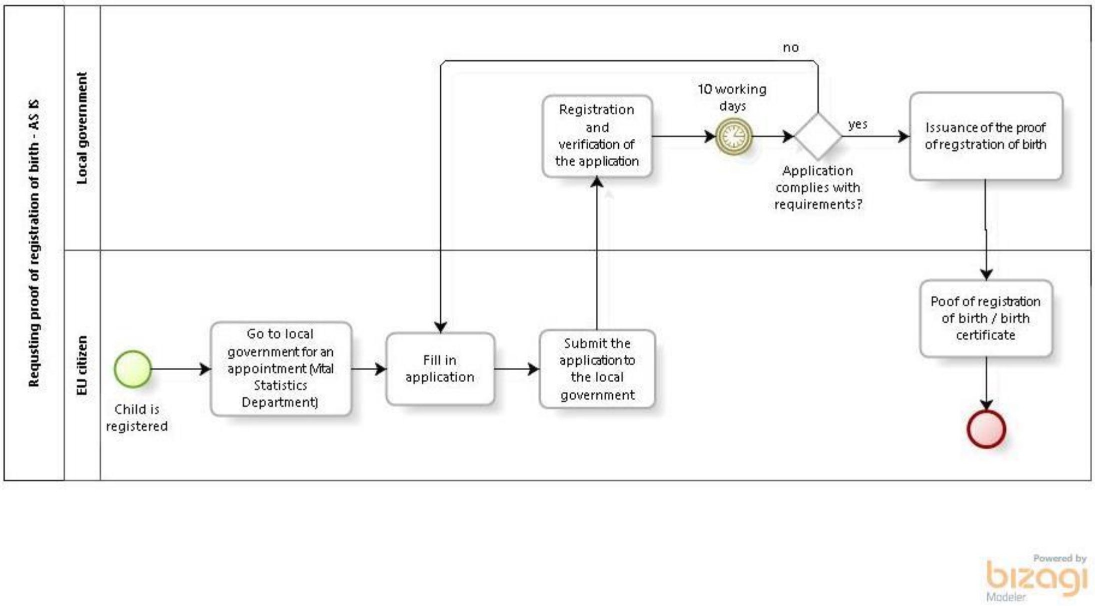
Requsting proof of registration of birth - AS IS
Local government
EU citizen
no
Registration and verification of the application
10 working days
yes
Application complies with requirements?
Issuance of the proof of reggstration of birth
Child is registered
Go to local government for an appointment (Vital Statistics Department)
Fill in application
Submit the application to the local government
Poof of registration of birth / birth certificate
Powered by bizagi Modeler

Figure 9. Requesting a proof of registration of birth – overall AS-IS process.

Estonian citizens can additionally request a proof of registration of birth using a fully automated online procedure available via e-population register. The Figure 10 describes the current application process for EE citizens.

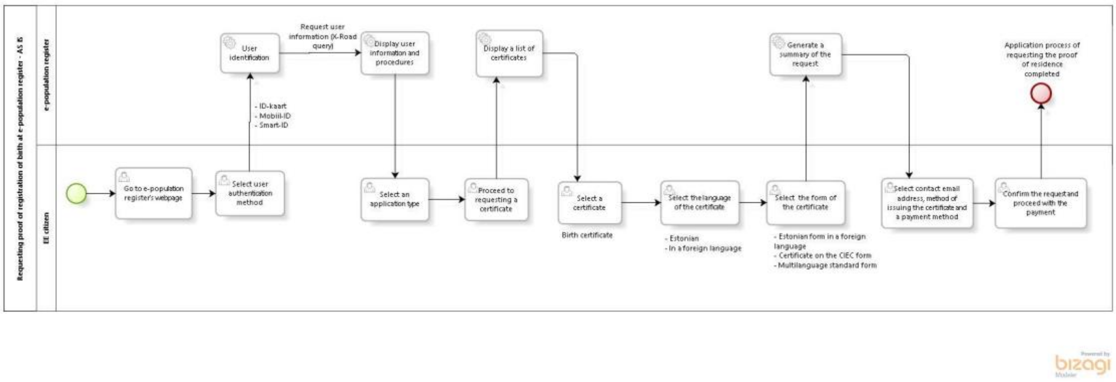
Requesting proof of registration of birth at e-population register - AS IS
e-population register
EE citizen
Go to e-population register's webpage
Select user authentication method
- ID-kaart
- Mobiil-ID
- Smart-ID
User identification
Request user information (X-Road query)
Display user information and procedures
Select an application type
Proceed to requesting a certificate
Display a list of certificates
Select a certificate
Birth certificate
Select the language of the certificate
- Estonian
- In a foreign language
Select the form of the certificate
- Estonian form in a foreign language
- Certificate on the CIEC form
- Multilanguage standard form
Generate a summary of the request
Select contact email address, method of issuing the certificate and a payment method
Confirm the request and proceed with the payment
Application process of requesting the proof of residence completed
Powered by bizagi Modeler

Figure 10. Requesting a proof of registration of birth at the e-population register – AS-IS process.

The process starts with a user identification at the e-population register http://www.rahvastikuregister.ee/ online portal. The user must choose between the eID means provided for authentication. After the register has successfully identified the user, the dashboard of information about the available procedures and documents will be displayed. In order to request a birth certificate, the user selects an application type and a certificate and proceeds with the application. Next, the user needs to select the language of the certificate – in Estonian or in a foreign language. In case the certificate was issued in a foreign language, the user must additionally select the form of certificate from one of the following options: 1) Estonian form in a foreign language, 2) certificate on the CIEC form, 3) Multilanguage standard form. After that, the system will generate an overview of the request, where the user will review the application. The user is asked to provide the preferred email address for sending any notices concerning the request. As one of the last steps, the user must select the method of issuing the certificate from one of the following options: 1) on paper from the local municipality government, 2) digital document sent via email in encrypted form, 3) on paper form a foreign mission. Finally, the user is requested to select a payment method for the state fee (internet bank / credit card payment). After confirming the request, the user will be directed to proceed with the payment. Once the state fee has been paid, the application process is completed and the user can monitor the status of the application in the dashboard [55]. Similar process could be adopted for requesting proof of residence.

Since the Estonian residence permit card has the digital component in the card, alike Estonian ID card, it provides an access to the desired online procedures. However, in order to issue the residence permit card, EU citizen must make two physical appointments. Alternatively, the EU citizen can access the online procedures using one of the EU eID means that are recognized by the EU member states [10]. At the time of signing in process, the digital public service providers use the X-Road to make a back-end query about the person, who attempts to sign in to check if the person with the identity code provided at the login process, exists in the population register. As currently there are no identity mapping procedures for EU identities, the access to the online procedure will be granted, but the access to online procedures will be limited or declined. Although, the EU eID authentication via eIDAS could have a lot of potential to minimize the physical number of contacts for accessing to the online procedures, it lacks a support of a trusted automated identity matching processes.

Although, there is an electronic format of submitting the application to issue a PIC, the current process foresees that a person must either way make a physical appointment to the public administration office in order for a physical identity verification. The following data must be submitted to the population registry (over the Estonian X-Road data exchange layer) upon the request of PIC:

- First name(s) at birth;
- Family name(s) at birth;
- Date of birth
- Gender
- Place of birth
- Citizenship
- Nationality
- PIC of the country of origin;
- A document proving the identity and citizenship (including: document type, number, date of issue, date of expiry, document issuer country);
- Name and legal identifier of the competent authority issuing PIC [54].

The bottleneck, in terms of cross-border service provision, appears to be at the first step of the process and is related to the identification and authentication of a foreign citizen. According to the interviews conducted with e-government experts, the UML diagram in Figure 11 consolidates the most common approach how the digital public services currently handle the authentication of a foreign or an EU citizen.

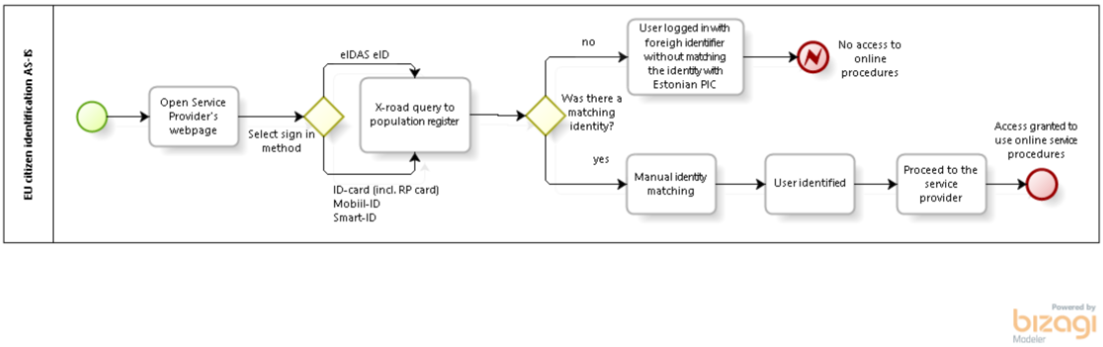
EU citizen identification AS-IS
Open Service Provider's webpage
Select sign in method
eIDAS eID
X-road query to population register
ID-card (incl. RP card)
Mobiil-ID
Smart-ID
Was there a matching identity?
no
yes
User logged in with foreigh identifier without matching the identity with Estonian PIC
No access to online procedures
Manual identity matching
User identified
Proceed to the service provider
Access granted to use online service procedures
Powered by bizagi Modeler

Figure 11. Authentication of EU citizen – AS-IS process.

The current approach lacks a central procedure for automated matching of the identities.

5.3.3 Requesting proof of residence: TO-BE

In light of the COVID-19 pandemic, the number of physical contacts on communication with public administrations should to be reduced. The automated processes in public online services can help to minimize the physical contacts. Citizens, but as well businesses and public administration, can benefit from it by saving up time and money spent on unnecessary bureaucracy. According to the mapping of the AS IS processes of the two case studies, the online procedure on requesting the proof of registration could adopt the AS IS process of the application on requesting a birth certificate. The proposed TO BE process is described in the Figure 12.

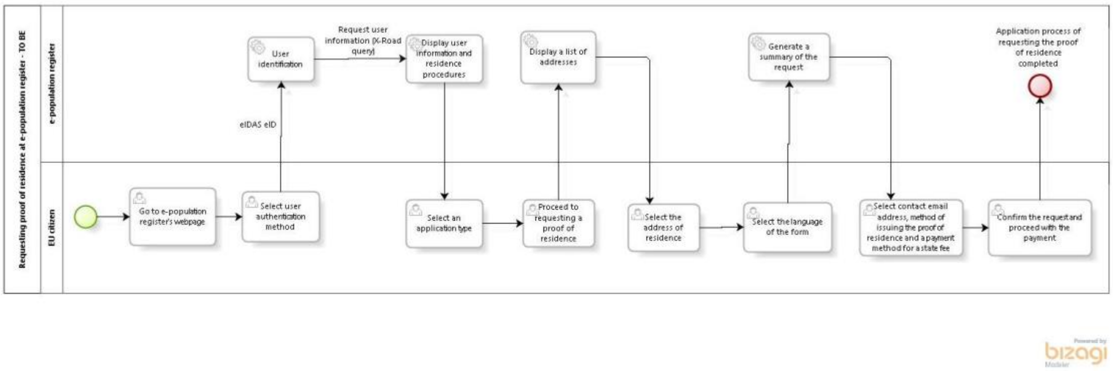
Requesting proof of residence at e-population register - TO BE
e-population register
EU citizen
User identification
Request user information (X-Road query)
Display user information and residence procedures
Display a list of addresses
Generate a summary of the request
Application process of requesting the proof of residence completed
eIDAS eID
Go to e-population register's webpage
Select user authentication method
Select an application type
Proceed to requesting a proof of residence
Select the address of residence
Select the language of the form
Select contact email address, method of issuing the proof of residence and a payment method for a state fee
Confirm the request and proceed with the payment
bizagi Modeler

Figure 12. Requesting a proof of residence at the e-population register – TO-BE process.

5.3.4 Requesting proof of registration of birth: TO-BE

According to the analysis of the AS-IS process presented in Figure 10, the same process could be adopted for EU citizens via e-population register, where no additional modifications for the service provision processes are needed. The e-population register provides a fully automated online procedure for a seamless user experience and complies with the vision of OOP. The UML scheme in Figure 13, is presenting the TO-BE application process for requesting a proof of registration of birth from the EU citizen perspective.

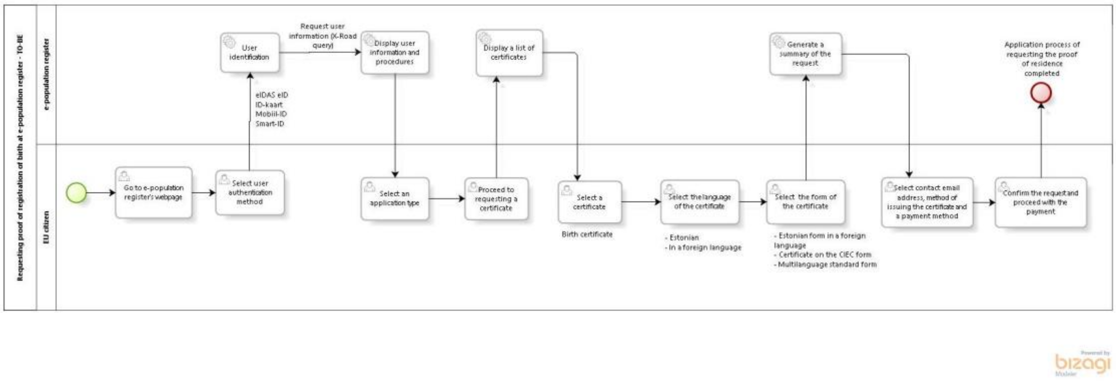
Requesting proof of registration of birth at e-population register - TO-BE
e-population register
EU citizen
User identification
Request user information (X-Road query)
Display user information and procedures
Display a list of certificates
Generate a summary of the request
Application process of requesting the proof of residence completed
eIDAS eID
ID-kaart
Mobiil-ID
Smart-ID
Go to e-population register's webpage
Select user authentication method
Select an application type
Proceed to requesting a certificate
Select a certificate
Birth certificate
Select the language of the certificate
- Estonian
- In a foreign language
Select the form of the certificate
- Estonian form in a foreign language
- Certificate on the CIEC form
- Multilanguage standard form
Select contact email address, method of issuing the certificate and a payment method
Confirm the request and proceed with the payment
bizagi Modeler

Figure 13. Requesting a proof of registration of birth at the e-population register – TO-BE process.

5.3.5 Proposed solution for identity matching

The central issue that the digital service providers are hoping to resolve in future, is to automatize the identity mapping procedures. The cross-border availability of attributes highly affects the reliability of identity matching mechanisms.

Considering the requirements identified in Table 3 and following the direction and current practices on identity matching in Europe [56], the following procedures in Figure 14 on identity matching could be adopted in Estonia:

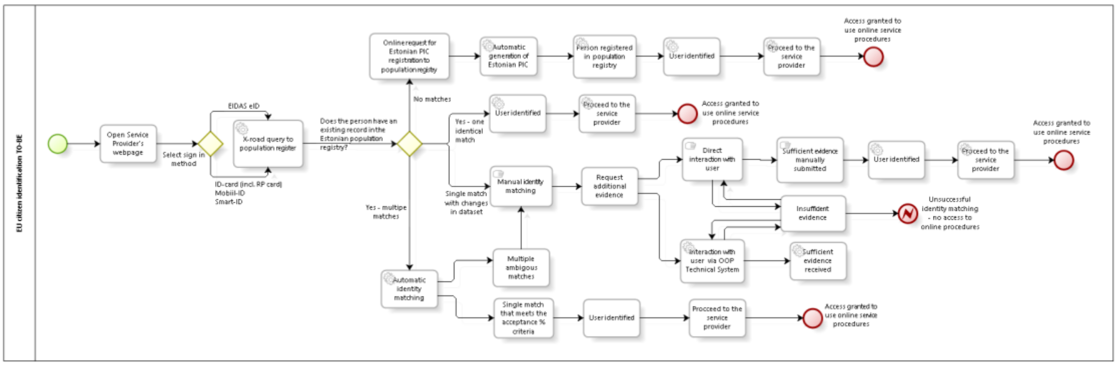
EU citizen identification TO-BE
Open Service Provider's webpage
Select sign in method
EIDAS eID
ID-card (incl. RP card)
Mobiil-ID
Smart-ID
X-road query to population register
Does the person have an existing record in the Estonian population registry?
No matches
Online request for Estonian PIC registration to population registry
Automatic generation of Estonian PIC
Person registered in population registry
User identified
Proceed to the service provider
Access granted to use online service procedures
Yes - one identical match
User identified
Proceed to the service provider
Access granted to use online service procedures
Single match with changes in dataset
Manual identity matching
Request additional evidence
Direct interaction with user
Sufficient evidence manually submitted
User identified
Proceed to the service provider
Access granted to use online service procedures
Insufficient evidence
Unsuccessful identity matching - no access to online procedures
Interaction with user via OOP Technical System
Sufficient evidence received
Yes - multipe matches
Automatic identity matching
Multiple ambigous matches
Single match that meets the acceptance % criteria
User identified
Procceed to the service provider
Access granted to use online service procedures

Figure 14. Authentication of EU citizen – TO-BE process.

In the UML scheme, an assumption is made that when a matching identity has been found, there is already an existing Estonian PIC assigned to the EU citizen. The centralized approach on identity matching system is recommended in order to reduce the burden for the service providers and increase the quality and reliability of the identity matching system. The approach of assigning a national identifier, such as Estonian PIC, to the eIDAS eID users helps to provide seamless user experience and enables automatic enrolment.

There are four scenarios where identity matching can be required:

1. First-time authentication: the service provider has no prior information in the population register of the user and the user has not been granted with Estonian PIC;

2. Recurring authentication: the user already exists in the population register and has been granted with Estonian PIC;

3. Recurring authentication with changed data set: some of the attributes in the data set has changed since the last authentication;

4. Cross-use of different eID means - the user has used different eID means to access the online procedures.

The key procedures involved in the proposed identity matching process are:

- Automatic procedure in case there is an existing identity with Estonian PIC that meets the following acceptance criteria:
    - the identifier used in authentication must be unique and persistent in time;
    - the user has provided sufficient attributes in the eID data set to perform reliable identity matching;
    - there has been a single match that meets the acceptance criteria of false positives;
- Manual procedure will be used in the following cases:
    - unsuccessful or false positive automatic matching results;
    - when additional evidence is requested from a user via direct interaction;
    - multiple ambiguous matches have been identified.
- The enrolment procedure to request Estonian PIC and entry to the population registry.

The main obstacle for cross-border automated data exchange that was mentioned throughout the interviews, was that many countries do not provide a unique identifier for natural persons alike in Estonia. For example, in Germany, each government authority assigns different identifiers to their citizens. That, in turn, requires the identity mapping procedure. In case the latter could be automatized, the cross-border data exchange could raise the data quality significantly.

5.4 Discussion

The analysis demonstrated several factors that influenced the seamless cross-border delivery of digital public services in Estonia. The discussion in this chapter will discuss the requirements and factors affecting the cross-border service delivery and will highlight the possible areas of improvement.

According to the findings from the literature of previous studies, documentation and interviews, the analysis proved the importance of interoperability in all the levels – legal, technical, semantic and organizational. The analysis confirmed the following barriers and factors that affect the cross-border interoperability of public services:

1. The complexity of the eID notification process slows down the recognition and, thereby, the accessibility to the digital services and procedures for EU citizens;

2. The lack of unique and persistent identifiers on the access to digital services;

3. Due to the limitations in national policies and law in many EU countries, the cross-border exchange of data and evidence of a natural person can be limited, which affects the overall success of the EU-wide adoption of the eIDAS and OOP in SDGR;

4. The lack of clear and standardized interoperability profile and reliable identity attributes in the EU on how to semantically describe the identities across registries;

5. Missing standardized and automatized approach on identity matching in the EU and national level. Since the identity matching highly relies on the existing records of a person in the base registries, the verification of EU eID users cannot be reliably performed without cross-border automated data exchange;

6. Different levels of assurance of eID means in EU affects the availability of cross-border services;

7. The e-government systems and national service providers cannot handle the format of foreign identifier, therefore the national identifier (PIC in Estonia) is a prerequisite for accessing the Estonian public services.

The documentation and thematic analysis identified a common issue of the current cross-border service provision concept across all the life events of the SDGR analyzed in this study – a lack of common understanding and non-existent standards for the identity management. The latter appeared to be the most crucial issue to the interoperability of EU digital public services. The findings of the case study confirmed the assumptions made on the analysis of theoretical and empirical data.

The key barriers on identity matching

In Estonia, public services are in general dependent on a unique and persistent identifier with a specific format. In EU, the format of a unique identifier varies from country to country, which has created an issue, where the service providers are unable to process foreign identities in their systems.

During the thematic analysis of interviews, it was pointed out that in order to automatize the process of identity matching, there should be internationally agreed standards how to semantically describe the identities across the registries. Therefore, the semantic interoperability could bring the identity mapping to a next level. In Estonia, there are currently only manual procedures in use for identity mapping, which does not support semantical interoperability between the databases and registries. Generating temporary identifiers in the registries for the foreign nationals will cause semantic inconsistencies between the national registries when the automatic data exchange comes along. One of the first and primary sources for the current identity mapping procedures rely on the data requested from the Estonian population register. The key requirement is that there must be an existing record in the population register to perform a secure identity mapping procedure. Since there is currently no common standardized identity mapping procedure in use for the base registries, the data exchange of a new incoming EU eID user is blocked over the X-Road.

During the analysis, the minimum data set requirements for mapping the identities of a natural person was pointed out, that includes the following attributes: first name(s), family name(s), PIC and date of birth. In some cases, the additional attributes are required, such as current address, country, gender, nationality and the place of birth. In many EU countries the current address is one of the most widely used additional attributes that are required in identity mapping process, but since not many countries are providing this attribute in cross-border scenarios, it is quite difficult to perform the mapping. This concludes that the efficient and reliable identity mapping should highly rely on the additional attributes that are persistent as possible in time.

Many EU countries do not provide a joint identifier for natural persons like in Estonia. For example, in Germany, each government authority assigns different identifiers to their citizens. As there is currently no unique identifier that has been widely adopted in EU, multiple workarounds or alternatives need to be implemented in cross-border scenarios to uniquely identify persons in order to avoid data breach and fraud.

5.4.1 Recommendations

Based on the research objectives, research questions and results of the analysis, the author provides the following recommendations and directions of improvement that are important from the aspects of seamless cross-border digital public service provision in Estonia.

Although, Estonia has widely digitalized its e-Government, the practical implementation of SDGR and eIDAS still raises various policy and security related issues. The commonly agreed interoperability profile and identity attributes in EU would therefore facilitate the exchange of basic information of natural persons.

In order to request additional evidence and attributes from authoritative sources in cross-border use case scenarios, the OOP technical system and eIDAS-Node could facilitate access to cross-border data. As the eIDAS regulation is currently under revision, the author suggests to consider the following:

1) The expansion of the mandatory eIDAS minimum data set attributes to improve reliable matching of identities. Ideally, the mandatory data set should consist of the attributes that are sufficient and persistent as possible in time, including: PIC, first name(s), family name(s), date of birth, country (as a prefix), current address, gender, nationality, place of birth;

2) The eIDAS eID notification procedure should emphasize the importance of unique identity attributes for cross-border use and, where it is possible, the unique identifier should ideally be the same for digital and physical eID to improve the reliability;

3) All the EU countries should consider notifying at least one eID scheme that meets the highest level of assurance to improve the accessibility and availability of cross-border public services.

Reusing the attribute information from base-registries is important for an efficient and user-centric cross-border service delivery. The exchange of cross-border attributes must be supported from technical, legal and semantical aspects.

The centralized approach on identity matching system is recommended in order to reduce the burden for the service providers and increase the quality and reliability of the identity matching. As presented in the cross-case synthesis and in the TO-BE model in Figure 14, the Estonian PIC can be used as a workaround for enabling the access with foreign eID to Estonian public services and online procedures. The approach of assigning a national identifier, such as Estonian PIC, to the eIDAS eID users helps to provide seamless user experience and enables automatic enrolment. However, some limitations apply with issuing Estonian PIC to foreign identities. The specific structure of Estonian PIC includes some information about a person that cannot be always provided with the current minimum data set of eIDAS eID, such as gender, but can be retrieved if the additional attributes are provided by the sending eID country.

6 Summary

The objective of the thesis was to identify the key barriers that prevent seamless digital service delivery of Estonian public services in cross-border use cases. The scope of this study focuses on a cross-border scenario where an alien with an eID from one of the EU Member States wants to access one of the Estonian digital public service procedures. To analyze how these barriers, affect the seamless service delivery in Estonia and to what extent the cross-border infrastructure should be improved, the TO-BE processes for specific and problematic areas were introduced.

To analyze the cross-border availability of Estonian digital public service procedures in the context of the SDGR, to understand the obstacles in cross-border service provision and the requirements behind it, the qualitative research approach was used along with case study methodology as the main methodology for this thesis. During this research, the evidence was collected using multiple sources and different data collection methods. For the analysis, several qualitative data analysis techniques were used. The selected methodology helped to find answers to the research questions.

In the first research question, which was divided into one sub-question, the author seeked to identify which are the main barriers in cross-border digital public service provision and how these barriers affect a seamless public service delivery in Estonia on a legal, organizational, technical and operational level.

According to the findings in previously conducted studies, over the past decade the EU has introduced various regulations and acts that directly apply to the EU Member States that has had an impact, not only on the national legislation, but also on the concept of cross-border interoperability and service provision. The literature review, document analysis and the empirical data analysis identified the main barriers that are preventing successful cross-border digital public service delivery in Estonia in legal, organizational, technical and operational level.

This research has identified that the cross-border digital service accessibility highly relies on the following factors: 1) secure identification, 2) cross-border functional and secure attribute exchange, 3) automatized identity matching based on sufficient attributes, 3) cross-border evidence exchange for specific procedures based on OOP technical system.

The main legal and organizational barriers identified in this study refer to the limitations in national policies and law in many EU countries, where the cross-border exchange of identity attributes remains limited or low. This affects the overall success of the EU-wide adoption of the eIDAS and OOP in SDGR. Another issue revealed during the study relates to the gaps in existing EU legislation that remain too general and, thereby, the implementation of EU regulations can be interpreted differently. The latter can become an additional barrier for a technical and operational level of interoperability. The complexity of the eID notification process in EU has been identified as potential constraint as the notification process is slowing down the mutual recognition of eIDs in EU and reduces the accessibility to the digital services and procedures for EU citizens. In the light of current eIDAS revision process, those key issues should be addressed to the EC.

The main technical and operational barriers identified in this study refer to the lack of clear and standardized interoperability profile with reliable identity attributes and standardized and automatized approach on identity matching in the EU. As the identity matching highly relies on the existing records of a person in the base registries, the verification of EU eID users cannot be reliably performed without cross-border automated data exchange. The lack of unique and persistent identifiers and different levels of assurance of eID means in EU affect the availability of cross-border services. As the e-government systems and national service providers cannot handle the format of foreign identifier, the national identifier (PIC in Estonia) is a prerequisite for the access to digital public services.

In the second research question, including one sub-question, the author presented the practical part of the research to understand the current state of play, the concepts and expectations of the cross-border service provision and how does the existing infrastructure support the cross-border digital public service delivery in Estonia. Based on the input obtained from the qualitative research data, the key requirements for a seamless cross-border service delivery in Estonia were formulated (see Table 3). The key requirements were validated through two case studies and a process improvement. The proposal of changes with recommendations for future implementations were presented in TO-BE processes in chapter 5.3.

As of 2020, the EC has opened a public consultation to re-evaluate the eIDAS regulatory framework with a goal to gather feedback from the member states about the existing drivers and barriers that impact of the current implementation and uptake of digital identity and trust services in EU [11]. The outcomes of the eIDAS revision are foreseen to set clearer direction towards a possible solution for the currently existing barriers.

6.1 Future direction

During the research, the author analyzed various constraints of the cross-border service provision in Estonia and provided recommendations how to overcome those obstacles focusing on the national perspective, but, as well, paying attention to the factors on the EU level that directly influence the success of a seamless cross-border service provision in Estonia.

This thesis provides a high-level foundation to continue with implementing the improvements proposed in TO-BE processes. For this, further analysis on the technical solution along with the proof of concept would be necessary.

Since the SDGR implementing regulation has not been adopted yet and the OOP technical system has not been released yet, the author sees a further need to analyze the cross-border service provision improvement in Estonia after the EC publishes the implementing acts and technical system.

In the recent years, the demand for cross-border services has increased, not only in the EU, but also outside the EU borders. Therefore, the analysis of the EU interoperability frameworks, such as eIDAS and SDGR, could be extended and analyzed in the context of third countries.

References

[1] V. Braun, V. Clarke, “Using Thematic Analysis in Psychology”, Article in “Qualitative Research in Psychology”, 3 (2), University of the West England: 2006. [Date accessed: 01.04.2020].

[2] EUR-Lex, “Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012”, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2018/1724/oj. [Date accessed: 12.01.2020].

[3] U. Flick, “An introduction to qualitative research”, (4th ed.), London: SAGE Publications Ltd: 2009. [Date accessed: 29.03.2020].

[4] J. W. Creswell, “Qualitative inquiry & research design: Choosing among five approaches”, (2nd ed.), Sage, Thousand Oaks, CA: 2007. [Date accessed: 21.04.2020].

[5] EUR-Lex, “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”, [Online]. Available: http://data.europa.eu/eli/reg/2014/910/oj. [Date accessed: 12.01.2020].

[6] EUR-Lex, “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”, [Online]. Available: http://data.europa.eu/eli/reg_impl/2015/1501/oj. [Date accessed: 12.01.2020].

[7] G. Aavik, “The Electronic Identification and Trust Service Regulation (EIDAS): An analysis of its Compatibility with the Estonian e-government System (EES)”, Master’s thesis, Tallinn: 2015. [Date accessed: 27.12.2020].

[8] Ministry of the Interior Republic of Estonia, “Residence Procedures”, [Online]. Available: https://www.siseministeerium.ee/en/residence-procedures. [Date accessed: 20.04.2020].

[9] Ministry of the Interior Republic of Estonia, “Population register”, [Online]. Available: https://www.siseministeerium.ee/en/population-register. [Date accessed: 20.04.2020].

[10] European Comission, “Overview of pre-notified and notified eID schemes under eIDAS”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS. [Date accessed: 12.04.2020].

[11] European Comission, “Trust Services and Electronic identification”, [Online]. Available: https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification [Date accessed: 02.04.2020].

[12] R. Bhattarai, “Analyzing the User Journey of Students of Member state to understand the Impact of Single Digital Gateway Regulation from citizens perspective”, Master’s thesis, Tallinn: 2019. [Date accessed: 27.12.2020].

[13] CEF Digital, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL. [Date accessed: 12.04.2020].

[14] Stibbe, “The new Regulation on electronic identification and trust services – eIDAS”, [Online]. Available: https://www.stibbe.com/en/news/2014/december/the-new-regulation-on-electronic-identification-and-trust-services--eidas. [Date accessed: 12.04.2020].

[15] J. W. Creswell, “Research design. Qualitative, quantitative and mixed methods approaches”, International student edition, Fourth edition, SAGE: 2014. [Date accessed: 29.03.2020].

[16] e-Estonia. [Online]. Available: https://e-estonia.com/. [Date accessed: 20.04.2020].

[17] CEF Digital, “Once Only principle (OOP)”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle. [Date accessed: 12.04.2020].

[18] European Comission, “The single digital gateway”, [Online]. Available: https://ec.europa.eu/growth/single-market/single-digital-gateway_en. [Date accessed: 12.04.2020].

[19] European Parliament, “Single digital gateway: a time saver for citizens and companies”, 12-07-2018, [Online]. Available: https://www.europarl.europa.eu/news/en/press-room/20180711IPR07739/single-digital-gateway-a-time-saver-for-citizens-and-companies [Date accessed: 12.04.2020].

[20] T. Puusaar, “KEY FACTORS INFLUENCING THE IMPLEMENTATION OF THE ONCE-ONLY PRINCIPLE: CASE STUDY OF ESTONIA”, Master’s thesis, Tallinn: 2019. [Date accessed: 15.04.2020].

[21] TOOP, “Once-Only”, [Online]. Available: https://toop.eu/once-only [Date accessed: 15.04.2020].

[22] TOOP, “Intensified collaboration with CEF”, [Online]. Available: https://toop.eu/node/376. [Date accessed: 15.04.2020].

[23] TOOP, “TOOP and the Single Digital Gateway”, [Online]. Available: https://toop.eu/sites/default/files/TOOP%20and%20SDGR_final.pdf. [Date accessed: 15.04.2020].

[24] T. Kalvet, M. Toots, A. van Veenstra, R. Krimmer, “Cross-border e-Government Services in Europe: Expected Benefits, Barriers and Drivers of the Once-Only Principle”, In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway, Ireland: April 2018 (ICEGOV’18), DOI: 10.1145/3209415.3209458. [Date accessed: 17.04.2020].

[25] M. Falch, R. Tadayoni, I. Williams “Cross-border e-Government Services in the Baltic Sea Region – Status and Barriers”, Article in Nordic and Baltic Journal of Information and Communications Technologies, 2018, (1):83-100, DOI: 10.13052/nbjict1902-097X.2018.006. [Date accessed: 17.04.2020].

[26] J. W. Creswell, “Qualitative inquiry and research design. Choosing among five different approaches”, Third edition, SAGE Publications Inc: 2013. [Date accessed: 16.01.2021].

[27] R. K. Yin, “Case study research and applications. Design and Methods”, Sixth edition, SAGE Publications, Inc: 2018. [Date accessed: 22.03.2021].

[28] H. Raamat, “Riiklik SSO (single-sign-on) ja Riigi autentimisteenus”, 2020, [Online]. Available: https://e-gov.github.io/TARA-Doku/files/SSO_esitlus_infopaev.pdf. [Date accessed: 01.01.2021].

[29] H. Hinsberg, K. Kala, L. Kask, A. Kütt, “Study on Nordic-Baltic Trust Services”, 04.11.2020, [Online]. Available: https://www.digdir.no/digitalisering-og-samordning/study-nordic-baltic-trust-services/2058. [Date accessed: 01.01.2021].

[30] S. Lips, N. Bharosa, D. Draheim, “eIDAS Implementation Challenges: the Case of Estonia and the Netherlands”, Electronic Governance and Open Society: Challenges in

Eurasia : 7th International Conference, EGOSE 2020, St. Petersburg, Russia, November 18-19, 2020, DOI: 10.1007/978-3-030-67238-6_6. [Date accessed: 04.01.2021].

[31] EUR-Lex, “Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) 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 (notified under document C(2015) 7369)”, [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_289_R_0007. [Date accessed: 22.03.2021].

[32] European Union, “New European Interoperability Framework. Promoting seamless services and data flows for European public administrations”, Belgium: 2017, [Online]. Available: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf. [Date accessed: 11.03.2021].

[33] European Comission, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS”, EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government, Brussels: 19.04.2016, [Online]. Available: https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation. [Date accessed: 13.04.2021].

[34] European Comission, “Moving forward with digital public services in Europe”, 2021, [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/moving-forward-digital-public-services-europe . [Date accessed: 15.04.2021].

[35] European Comission, “Ministerial Declaration on eGovernment - the Tallinn Declaration”, 2017, [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration. [Date accessed: 15.04.2021].

[36] CEF Digital, “eIDAS eID Profile”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile. [Date accessed: 21.04.2021].

[37] P. Runeson, M. Höst, A. Rainer, B.Regnell, “CASE STUDY RESEARCH IN SOFTWARE ENGINEERING. Guidelines and Examples”, John Wiley & Sons, Inc: 2012. [Date accessed: 20.04.2021].

[38] CEF Digital, “e-Identification”, [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/e-identification. [Date accessed: 22.04.2021].

[39] CEF Digital, “eID Documentation”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030 [Date accessed: 22.04.2021].

[40] N. J. Salkind, “Encyclopedia of Research Design”, SAGE Publications: 2010. DOI: https://dx.doi.org/10.4135/9781412961288. [Date accessed: 30.04.2021].

[41] J. R. Frade, “The Once Only initiative – a stepping stone to Europe’s recovery”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Initiative%3A+Towards+Cross-Border+Connectivity. [Date accessed: 01.05.2021].

[42] Digital ID Working Group of the Secure Identity Alliance & Onepoint, “Giving voice to digital identities worldwide. Key insights and experiences to overcome shared challenges”,

2021, [Online]. Available: https://secureidentityalliance.org/utilities/news-en/entry/giving-voice-to-digital-identities-worldwide-1-1. [Date accessed: 01.05.2021].

[43] e-Estonia, “X-Road”, [Online]. Available: https://e-estonia.com/solutions/interoperability-services/x-road. [Date accessed: 01.05.2021].

[44] e-Estonia, “Population Registry”, [Online]. Available: https://e-estonia.com/solutions/interoperability-services/population-registry. [Date accessed: 01.05.2021].

[45] Information System Authority, “Data Exchange Layer X-tee”, [Online]. Available: https://www.ria.ee/en/state-information-system/x-tee.html. [Date accessed: 01.05.2021].

[46] Information System Authority, “The Information System Authority’s authentication services”, [Online]. Available: https://www.ria.ee/en/state-information-system/eid/partners.html#tara. [Date accessed: 01.05.2021].

[47] TARA-Doku, “Riigi autentimisteenus”, [Online]. Available: https://e-gov.github.io/TARA-Doku/. [Date accessed: 02.05.2021].

[48] Information System Authority “Electronic Identity eID”, [Online]. Available: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html. [Date accessed: 02.05.2021].

[49] Eurosmart, “Implementation of the eIDAS nodes: State of play”, 03.09.2020, [Online]. Available: https://www.eurosmart.com/implementation-of-the-eidas-nodes-state-of-play/. [Date accessed: 05.05.2021].

[50] eIDAS Technical Sub-group, “eIDAS SAML Attribute Profile. Version 1.2”, 28.10.2016, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile?preview=/82773108/148898847/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf. [Date accessed: 05.05.2021].

[51] CEF Digital, “How can Identity Matching improve the experience of citizens on online public services?”, [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/06/27/How+can+Identity+Matching+improve+the+experience+of+citizens+on+online+public+services. [Date accessed: 06.05.2021].

[52] Deloitte, “Study on Data Mapping for the cross border application of the Once-Only technical system SDG. D04.01 – Final Report”, 28.02.2020, [Online]. Available: https://sdg.mindigital.gr/uploads/Deloitte_final_report.pdf. [Date accessed: 06.05.2021].

[53] Ministry of the Interior Republic of Estonia, “Vital Statistics Procedures”, [Online]. Available: https://www.siseministeerium.ee/en/vital-statistics-procedures. [Date accessed: 08.04.2020].

[54] Riigi Teataja, “Isikukoodide moodustamise ja andmise kord”, [Online]. Available: https://www.riigiteataja.ee/akt/108012019011. [Date accessed: 09.05.2021].

[55] Ministry of the Interior, e-population register, [Online]. Available: https://www.rahvastikuregister.ee/. [Date accessed: 09.05.2021].

[56] H. Leitold, “eIDAS Identity Matching in Austria”, CEF Identity matching Webinar: 24.04.2019, [Online]. Available: https://pure.tugraz.at/ws/portalfiles/portal/26511342/20190424_Webinar_AT_Identity_Matching.pdf. [Date accessed: 09.05.2021].

Appendix 1 – Interview questions

1. Are the public services you provide in your area available for foreign eID users today?
2. What is the minimum data set that is required to access your digital public services and procedures for natural and legal persons? Is the data set required available in the government base registers?
3. Which government base registers do you use as a data-providers for your digital public services?
4. Does any of the digital public services in your area require digital signing?
5. The eIDAS Regulation defines three levels of assurance for the use eIDs cross-border: Low, Substantial and High. Which of the aforementioned eID assurance levels do you accept or are willing to accept in your digital public services for cross-border use?
6. Do you use any specific methodology for the risk evaluation for the levels of assurance in your digital public services? Please describe the current practices.
7. What are the current practices you use today for identity mapping and verification of foreign citizens in your systems? Please describe the current practices (if any) or refer if there are any initiatives planned for this?
8. Are there any cross-border interoperability solutions planned or already deployed that support cross-border service provision in your area (e.g. for document exchange, electronic identification or data and evidence exchange)? Please refer to the initiatives and the selection criteria of cross-border interoperability solutions (if any) and how they fulfill the business needs in your area?
9. Which are your expectations and requirements for the cross-border interoperability solutions in the business level in your area?
10. Which are your expectations and requirements for the cross-border interoperability solutions from the technological perspective in your area?
11. How would you evaluate efficiency and necessity of the existing cross-border interoperability solutions and ongoing initiatives for the digital public service provision in your area? Which are the deficits you have identified so far?