TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Karolina Bejussova 204718IVGM

Assessment of the eID Ecosystem as a Part of the State`s Critical Infrastructure: the Case of Estonia

Master's thesis

Supervisor: Silvia Lips
LL.M, MSc

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Karolina Bejussova 204718IVGM

eID ökosüsteemi kui riigi kriitilise infrastruktuuri osa hindamine: Eesti juhtumiuuring

Magistritöö

Juhendaja: Silvia Lips
LL.M, MSc

Tallinn 2022

Author’s declaration of originality

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

Author: Karolina Bejussova

09.05.2022

Abstract

Nowadays, in the era of digital transformation, electronic identification (eID) is a cornerstone of the electronic country`s state in the electronic service (e-service) delivery and information exchange between the government with its citizens and businesses. Thus, a secure and reliable eID is significant to prevent the risk of privacy and vulnerability by focusing on the quality and resilience of eID in delivering high-value e-services.

This thesis aims to present the assessment of eID and the ecosystem around it as a part of the state`s critical infrastructure (CI). Based on the Estonian case, this thesis aims to identify the readiness of the eID ecosystem to become essential for society to facilitate eID resilience and protection.

Since 2017, digital identification and digital signing in Estonia have been considered a part of the state`s CI. In this thesis, the Estonian case has been chosen as the main methodology along with the qualitative data collection techniques to research a new phenomenon of the eID vital significance.

During the research, the concept of CI was investigated in application to the eID ecosystem. The thematic analysis was adopted to analyse primary data collected by conducting semi-structured interviews with Estonian experts in the eID field.

As a result of this research, the author provided an explanatory checklist for assessing the eID ecosystem as a part of the state`s CI to facilitate eID resilience and critical infrastructure protection.

This thesis is written in English and is 65 pages long, including 9 chapters, 9 figures and 4 tables.

Keywords: electronic identification, critical infrastructure, resilience, critical elements, critical infrastructure protection, eIDAS.

List of abbreviations and terms

CI	Critical infrastructure
CII	Critical information infrastructure
CIIP	Critical information infrastructure protection
CIP	Critical infrastructure protection
E-governance	Electronic governance
E-government	Electronic government
eID	Electronic identification
eIDAS	Electronic Identification, Authentication and Trust Services
E-service	Electronic service
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
OECD	Organization for Economic Co-operation and Development
PBGB	Estonian Police and Border Guard Board
PKI	Public Key Infrastructure
PPP	Public-Private Partnerships
RIA	Estonian Information System Authority
ROCA	Return of the Coppersmith Attack
SMIT	IT and Development Centre

Table of contents

List of figures

List of tables

1 Introduction

1.1 Background

Nowadays, in the digital era, Information and Communication Technologies (ICTs) made significant changes in digital transformation. Technological capabilities provided a significant contribution to the way of government, organizations, and businesses can operate. The use of ICT significantly changed social perception with public awareness and increased opportunities for the service delivery process.

In the era of digital transformation, technological development with ICT usage has led to a rise of web-based services and digital government solutions in the public sector management process provided by government institutions in different countries (Asgarkhani, 2005). Furthermore, the use of ICT brought a new value to public management transformation, where electronic governance (e-governance) meets society's demand for social and economic development. Based on interaction with ICT, e-governance enables the government to establish a more valuable relationship with its citizens and businesses (Asgarkhani, 2005).

However, the concept of interaction with the government by delivering and providing public digital or electronic services (e-services) may provide different challenges. This research focuses on digital identity or electronic identification (eID). eID is an essential part of any government` with a mature e-governance ecosystem, where the identity ecosystem presents a new concept, in which different entities, such as individuals, private and government organizations provide a significant impact (Rasouli et al., 2021).

Achieving eID and its management has been identified as a core element for the e-governance ecosystem that includes, for instance, infrastructure, e-services, processes, and interoperability framework (Lips et al., 2019). eID is a cornerstone of the electronic state in the e-services delivery process and information exchange between the government with its citizens and businesses in an advanced digital society.

Although a person`s identity might have different clarities, however, it is crucial to differentiate paper-based identification systems from identification practices and designs used in the digitally networked world. Camp (2003) stated that to prevent vulnerability in the identity designing process, it is significant to clarify and understand the clarity of identity and interaction of its elements in the digital system. Rasouli et al. (2021) stated that identity privacy is one of the concerns of digital identity. Thus, a resilient and reliable eID and its ecosystem play a significant role as a digital solution that allows secure online authentication, enables digital signatures with data encryption, and facilitates personal public e-services with a secure data exchange process.

Although this thesis investigates a particular case of Estonia, however, this research focuses on the electronic identity system, called eID, which is considered a substructure to provide electronic government (e-government) services and other e-services. eID is used to perform electronic activities and daily operations based on an official identity document, such as accessing daily e-services and giving digital signatures.

1.2 Research purpose

The purpose of this research is to present the assessment of eID and the ecosystem around it as a part of the state's critical infrastructure (CI). The project aims to identify the readiness of the eID and its ecosystem to become an essential state asset, which facilitates vital services for the functioning of a society and state economy.

The research focuses on the Estonian case, which has been chosen as one of the most successful and highly developed cases in the field of eID and its ecosystem. Since 2017, in Estonia, according to the Emergency Act (Riigikogu, 2017), Estonian eID, namely digital identification and digital signing, have been considered a part of the state's critical infrastructure. Thus, digital identification and digital signing in Estonia equate to other vital services, such as electricity supply, natural gas supply, operability of national roads, and phone services. The principle aim of the chosen Estonia as a case study is to learn more about digital identity, which facilitates citizens' daily transactions in the public and private sectors through its experience and challenges.

During the research, the critical infrastructure components are investigated in the application of eID to identify its critical elements. Conducted interviews focused on the

Estonian case by investigating requirements and preconditions of the eID ecosystem that are necessary to become a part of the state`s critical infrastructure.

Based on the Estonian case analysis, as a result of this research, the project seeks to provide a solution to show how the state can identify whether eID and its ecosystem are ready to become considered critical.

1.3 Research motivation

The idea of the research topic starts from the previous research papers, which show the significance and demand of digital identity for the development of the digital economy and high-value electronic services. Online services are more at risk of privacy, trust, and security, in which a trustworthy, secure, and reliable digital identity is significant to prevent system vulnerability, threats to individual safety, and national security (Perez, 2021). eID as a part of the critical infrastructure is a relatively new phenomenon, which encourages in-depth research. The research results may significantly contribute to critical infrastructure protection and contribution to the digital economy with further research ideas.

Also, a secure digital identity transforms business practices into a safe remote way, which provides more opportunities in the service delivery process and new business models (Al-Khouri, 2014). Therefore, it is significant to approach quality and resilience in a digital system by rethinking the digital identity landscape and framework. Critical benefits and positive impacts can be achieved by treating and protecting eID as a part of the state`s critical infrastructure.

In addition, the COVID-19 pandemic made a significant impact on our society, which accelerates the need for online public and private services worldwide. Beduschi (2021) proposed the demand to build digital identity solutions based on data privacy and the human rights approach, which might strengthen the digitalization process. Therefore, the pandemic increased the demand for protection systems, where eID plays a crucial role in sustaining digitality within social protection systems (Masiero, 2020). Thus, treating eID as a part of the critical infrastructure may shape the technical, legal, and ethical standards by approaching resilient systems against failure, which can be adopted by developing and developed countries.

The motivation of the chosen Estonia as a case study starts with the fact that in Estonia, the usage of eID is relatively high. In Estonia, eID plays a vital role in enabling secure access to public and private e-services. According to the E-Governance Academy (2016) report, 99% of bank transfers are done electronically in Estonia. Also, through the e-Tax board, 98% of tax returns are done online, and 95% of prescriptions are done using a digital prescription system. Lips et al. (2018) stated that Estonian practice is a good example of effective management to handle the proposed, in their research, electronic identity security issue crisis by relying on technological advances, public-private partnership, and openness. Therefore, the author decided to bring the Estonian case as the best example of one of the world's most digitally advanced societies.

1.4 Research questions

This research aims to answer one main research question (RQ), which, in turn, is divided into three supportive sub-questions (SQ).

RQ: How is it possible to identify that the eID ecosystem is ready to be a part of the state's critical infrastructure?

Having assessed the case of Estonia, the main research question seeks to provide an explanatory solution, which will be used to identify the readiness of the eID ecosystem to become a part of the state's critical infrastructure.

To answer the main research question, the following three sub-questions are presented by creating a series of research steps to focus on research areas, which are:

SQ1: What are the eID critical infrastructure components?

SQ2: How did the eID ecosystem become a part of the Estonian state's critical infrastructure?

SQ3: What are the design requirements and preconditions necessary to become a part of the state's critical infrastructure?

Section 4 describes the methodology, which has been applied to this research by approaching the main research question and sub-questions to achieve the aim of the proposed research project.

1.5 Thesis outline

This thesis is divided into nine chapters. The first and present chapter gives an introductory overview of the topic by describing its background and purpose, followed by justified research motivation and research questions. The second chapter provides an overview of the existing literature on the research topic. The third chapter conceptualizes the background of theoretical design for critical infrastructure assessment by focusing on its key factors. The fourth part introduces the methodological approach by explaining the chosen research strategy, including collection and data analysis methods. The methodological part is followed by a fifth chapter of the case description.

The second part of the thesis presents research results and findings in chapter six, followed by the discussion part in chapter seven. The discussion part also includes recommendations provided by the author. Research limitations and future research direction is described in chapter eight and concluded by the summary in chapter nine.

2 Literature review

The current research topic focuses on two main fields, namely the eID ecosystem and critical infrastructure. Both subjects are broad, and different research papers are available for both fields in different contexts. The idea of combining and exploring these fields within one case study makes the topic even more unique. This chapter aims to provide a justified review and background of the available literature concerning the research topic.

To begin with, the proposed aim of the research project requires starting by providing a theoretical background by conceptualizing insights into what constitutes critical infrastructure, which will be applied to the specific case of the eID ecosystem. Having assessed existing research on the CI topic, the author can state that CI is a broad and complicated subject, which shows its significance in various concepts, contexts, and fields. CI has been studied in the contexts of its critical elements, resilience management, and protection purposes, which are based on complex theoretical approaches that are designed and applied for different CI fields and case studies.

CI is a complex system. The term infrastructure has been understood as a structure utilized for the provision of services or goods by humans, in which the term critical implies importance to society (Fekete, 2012). At a global level, there are no clear boundaries and well-defined terms on what constitutes CI, and, as a result, it does not allow direct identification of CI elements (Newbill, 2019). However, the disruption or failure of CI would have a significant impact on the economy, state interest, and society's well-being. Therefore, resilience in a CI system plays a substantial role in CI protection (Rehak et al., 2018). There are different beneficial methods presented to assess resilience in CI to contribute to sustainable and reliable infrastructure. For instance, Rehak (2020) proposed an ASOR method to assess and strengthen organizational resilience based on defining, assessing, and strengthening organizational resilience factors. Also, the CIERA method has been designed for assessing the CI technical and organizational resilience of elements by evaluating their robustness, recoverability, and adaptability (Rehak et al., 2019).

The complexity of the CI topic has also been identified by the process of designation of CI elements based on common criticality criteria (Popescu & Simion, 2012), which is a part of the management process of CI protection (Rehak et al., 2018). There are different papers which focus on providing an approach to identifying critical elements. For

instance, Leitner et al. (2017) provided a method to identify CI elements in the railway sub-sector of the transportation sector. Novotny and Janosikova (2020) brought a progressive bottom-up approach to identify regional CI elements through its failure impact assessment, which the researchers applied to the case of the road infrastructure of the Czech Republic. Also, Fekete (2012) aimed to develop criteria based on a top-down type of assessment to identify what is critical for society, which can be applied to different infrastructures.

Brunner and Suter (2008) stated that one of the primary purposes is to attempt to better and secure CI, where critical infrastructure protection (CIP) is a crucial part of national security. It was noted that CIP is a long-term issue based on sustainable development (Rehak et al., 2018), where each state is responsible for CI protective measures (Newbill, 2019). However, some approaches have been mentioned in CIP in the scientific world. For instance, the Public-Private-Partnerships (PPP) approach has been studied by approaching the enhancement of the economic value and improving the efficiency of infrastructure delivery (Cui et al., 2018). Medaglia et al. (2017) investigated the banking sector's involvement in the development of eID in the case of Denmark. Also, Cavelty and Suter (2009) studied the usefulness and limitations of PPP for CIP based on the network approach developed by governance theory.

Having gained knowledge in the CI field, the author can focus on the eID and research the case in application to the CI theoretical background. The concepts of eID and electronic signatures are crucial for transactional e-government service. The recent research papers showed demand for more efficient and trustworthy digital identity systems in public and private sectors.

The author found different research papers on the digital identity field in different contexts. For instance, Beduschi (2021) proposed a data-privacy centric and human rights-based approach for a digital identity solution as the best way to strengthen the process of digitalization. Rasouli et al. (2021) studied the most critical factors of digital identity management by proposing a framework that can manage digital identity in cyberspace. Also, Mir et al. (2020) conducted a study to identify the key priorities for designing the national biometric identity system based on a single case study.

Estonia is one of the leading electronic states, which has already become a case of various research papers. According to Lips et al. (2019), eID has been studied in a way of designing a long-term identity management strategy for a mature electronic state with a high e-governance maturity level, which is supported by the research on a security vulnerability, where the Estonian case of worldwide cryptography vulnerability (the ROCA case) was investigated (Lips et al., 2019). The ROCA case in Estonia became a part of the valuable in-depth analysis of the crisis management process implicated by large-scale security risk, which can provide input for the other countries to improve the existing environment while developing the eID system based on the citizens' rights (Valtna-Dvořák et al., 2021). In addition to authentication, digital signing, and encryption, the Estonian eID card showed its uniqueness, for instance, in the use of loyalty programs purposes. Morgan and Parsovs (2017) investigated the risks of the authentication mechanism of ID card chips, which facilitates the further development of secure and universal solutions.

In addition, having considered the research area of eID in the security context, as an impact of the cyber crisis in Estonia caused by a vulnerability in 2017, Parsovs (2020) researched legal issues caused by the lack of technical preparedness, time pressure, and situation criticality. The case is also supported by the research showing how to improve the security and usability of user identity on the Internet, based on working solutions in Estonian practice (Parson, 2013).

There are different research papers available in both the eID and CI fields. According to the findings, it might be stated that different countries seek to attempt secure, trustworthy, rights-based, and data-privacy centric eID. Reliable eID will strengthen the process of digitalization and provide a stable long-term strategy in the e-governance field. The approach of assessing eID as a part of the critical infrastructure will significantly impact the development and sustaining of eID and its ecosystem by focusing on security and protection. Having reviewed the Estonian case, it might be stated that the rich Estonian background can significantly contribute to the chosen research topic.

3 Theoretical framework

This chapter focuses on the overview of the available related studies and theories considering the concept of critical infrastructure, on which this study relies as a theoretical framework. This section aims to identify the relevant factors concerning critical infrastructure.

3.1 Defining critical infrastructure

To begin with, it is significant to define the concept of critical infrastructure. For instance, some official documents state that CI is the backbone of modern economies consisting of crucial systems and services, such as financial and technology systems, telecommunications, energy, and water supply (Organization for Economic Co-operation and Development [OECD], 2019). Also, CI is recognised as physical or virtual assets, systems, networks, or thereof designed to facilitate the provision of essential goods and services (Council of the European Union, 2008).

Also, both definitions from OECD and the European Union Council stated that CI systems provide vital resources and services that are mainly important for society and state interests. As a result of the failure, the disruption or destruction of such vital resources or services would influence economic and social well-being, health, security, and social functions. Thus, resilience in a CI has a significant impact, which provides quality to reduce vulnerability and facilitates adaption to disruptive events (Rehak et al., 2018).

However, since the mid-1990s, many studies have been concerned with defining critical infrastructure, which has changed in different nation-states over time. Since time progress and technological advancement, the list of industries and critical infrastructure sectors has expanded. Having researched the CI definitions, Newbill (2019) stated that there is a concern in defining the rigorous and overarching definition of CI due to variations of criticality criteria between different nation-states and systems that constitute CI throughout the world. Also, for instance, European Union CI Protection Model does not let identify CI elements at the regional level due to focusing on European and national levels (Novotny & Janosikova, 2020).

Estonia is a member of the EU. Therefore, Estonia interprets the concept of CI as indicated for the Member States in the Council of the European Union (2008). Thus, in the research project, CI defines as essential for the maintenance of vital societal functions, health, safety, security, economics, an asset, system, or part thereof, the disruption of which, as a result of the maintenance failure, would have a significant impact on social well-being.

3.2 Elements

Critical infrastructure is a comprehensive system. To identify whether infrastructure or asset is critical for society, it is significant to identify critical infrastructure components by looking at, for instance, the infrastructure components or nodes, customer needs, capabilities of organizations, and mitigation resources, based on common and appropriate criticality criteria to show what might become critical (Popescu & Simion, 2012). Identifying CI elements is proposed as an initial stage of protecting CI by applying comprehensive security measures to strengthen their resilience (Novotny & Janosikova, 2020). According to Rehak et al. (2018), Figure 1 represents the management process of CI elements protection, where the designation of CI elements is an initial step of protection management. There are different approaches to identifying CI elements and conceptualising CI based on various assessment approaches.

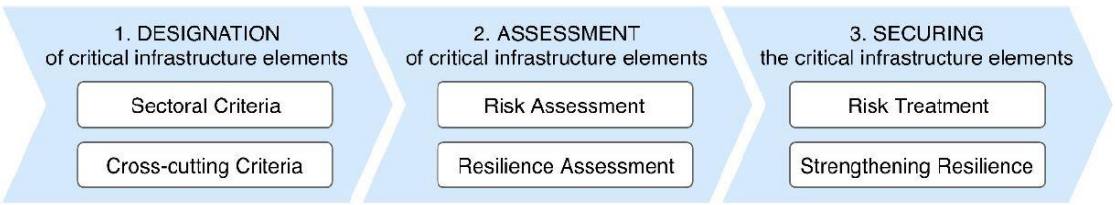

Figure 1. Critical infrastructure elements management process (Rehak et al., 2018).

Although the CI approach integrates many similar approaches, there are different ways to structure and conceptualize CI. Fekete (2012) mentioned that criticality assessments are similar to risk assessments aiming to identify risk spots, which can be conducted using top-down or bottom-up element evaluation. Fekete (2012), in the research paper, provided one of the ways of describing common criteria and infrastructure components. It is based on the top-down type of assessment applied to a wide range of infrastructures to identify and evaluate infrastructure regarding its criticality to society. The researcher proposed

three criticality criteria, which integrate characteristics of CI, such as critical proportion, critical time, and critical quality. The following illustration in Figure 2 contains possible examples of such criteria and the applications that the researcher proposed.

Generic criterion	Examples of specific criteria	Examples of applications (many criteria are valid for almost all types of infrastructure)
Critical proportion	Load, capacity, power, sales, turnover, etc.	Traffic, logistics chains, power installed
	Number of assets, nodes, interdependencies, redundancies, emergency capacities	Backup systems for power or information storage; emergency power
	Amount of customers supplied	For instance, the number of people supplied with drinking water
	Outreach / spatial interconnectedness	The single chemical plant in the world producing a key product
Critical time	Failure duration	Air traffic grounding due to volcanic ash
	Mean time to repair, replace, restore the functionality	Replacement time for a transformer station
	Mean time to react	Police, fire brigade, medical units, media, early warning, crisis management
	Timing of failure	Coldest winter day; annual meeting of company leaders; day of distribution of welfare or pay checks
Critical quality	Product or service quality	Water or food quality, trust in finance, training of staff, feeling of security
	Cultural or societal significance	National cultural icons

Figure 2. Criteria for various infrastructure types (Fekete, 2012).

The bottom-up approach allows the optional implementation of individual criteria and preferences, while the top-down way utilizes cross-cutting and sectoral criteria based on national and European CI elements (Novotny & Janosikova, 2020). In addition, the researchers proposed a progressive systemic approach based on bottom-up element evaluation across the whole system, which applies to different countries at the regional level for both public and private sectors. The proposed approach consists of processes within four phases, which are equivalent to the risk management framework for increasing security and preparing the whole area for the crisis.

In this research, to identify eID critical infrastructure components, the author has chosen to follow the idea of Fekete's (2012) model, which is valid for many infrastructures and integrates typical characteristics, by looking for critical common factors, such as proportion, time, and quality in the process of crisis to determine, which elements have the significant impact on vital functions of the society due to the disruption event.

3.3 Resilience

In a concept of CI, resilience can be viewed as a quality that reduces vulnerability by representing internal preparedness for emergencies affected by internal or external disruptive factors. Resilience, in CI, is a crucial factor, which determines the reliability of its elements to respond, recover, and adapt to potentially disruptive events to avoid

negative impacts on the population (Rehak et al., 2018). In this regard, resilience management is crucial to identify weaknesses. Therefore, considering infrastructure systems' interdependence, resilience assessment plays an essential role in risk management to ensure the security and reliability of the CI elements and the whole system.

According to Rehak et al. (2018), resilience in CI is a cyclic process of prevention, absorption, recovery, and adaption improvements towards disruptive events. Figure 3 explains the resilience process in one cycle by continually improving absorption, recovery, and adaption processes. The difference between the original and new levels represents the degree of resilience improvements.

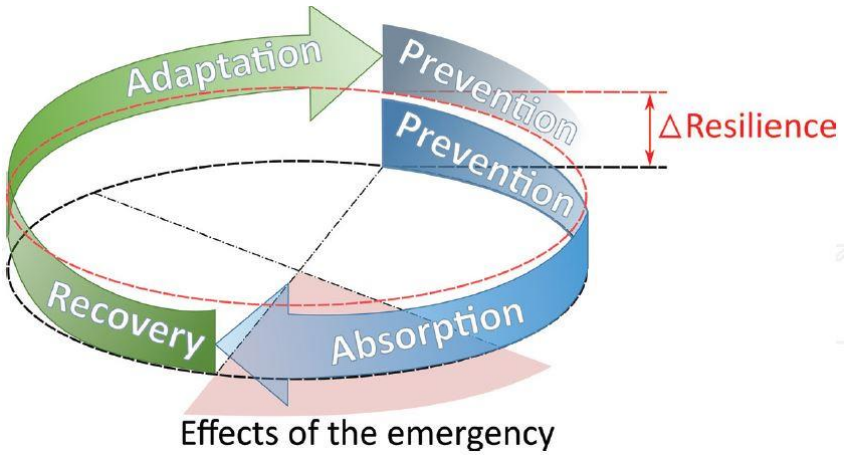

Figure 3. Critical infrastructure resilience cycle (Rehak et al., 2018).

Having researched resilience assessment of CI, it might be stated that in CI, systems resilience should be assessed at two levels, such as technological and physical, known as technical resilience of CI elements and organizational resilience of CI entities (Rehak, 2020). Figure 4 represents resilience components and their variables of two levels.

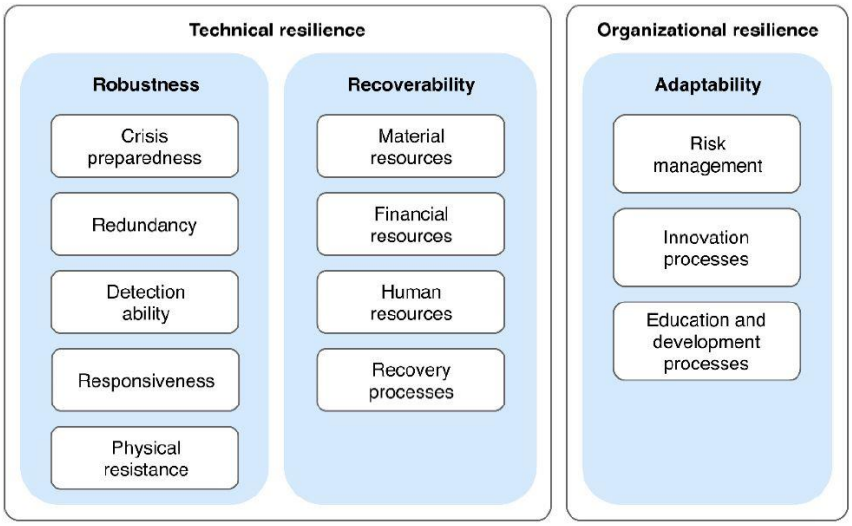

Figure 4. Critical infrastructure resilience components and variables (Rehak, et al. 2018).

Rehak et al. (2019) proposed the CIERA methodology, which states for Critical Infrastructure Elements Resilience Assessment. The proposed complex method is based on a quantitative assessment of the resilience of separately selected CI elements by evaluating their robustness to absorb the impacts of disruptive events, recoverability of functionalities after disruptive events, and adaptability to previous disruptive events. This method has been designed for technically oriented sectors, including technical and organizational assessments to strengthen the element`s resilience by identifying its weak points.

The organisational resilience assessment aims to strengthen organizational resilience in a CI system against any disruptive event by surviving in times of crisis and adapting to changing environments. Rehak (2020) proposed the ASOR method that applies to any CI entity and is formed for all CI elements operated by the organization, which states for Assessing and Strengthening Organizational Resilience. This method focuses on three basic processes that contribute to strengthening and organizational adaptability, such as risk management, organizational innovation processes, and education with development processes. The researcher states that compared to other studies, the advantage of this method is to focus on the positive impact of strengthening organization resilience individual factors, rather than assessing only technical resilience or using only a qualitative approach.

The research shows various theories available to assess the resilience of CI elements. However, the purpose of this thesis does not require an in-depth resilience or vulnerability

assessment of such components since this research does not approach a qualitative analysis. This research will use the idea of technical and organizational resilience components provided by Rehak et al. (2018) to determine the possible factors, which reduce the vulnerability of the eID critical components in the concept of CI.

3.4 Protection

Many countries worldwide seek to attempt better and secure CI, where critical infrastructure protection (CIP) is a crucial part of national security (Brunner & Suter, 2008). In different scientific fields, the issue of CIP concerning the long-term sustainable development of society has long been a research subject (Rehak et al., 2018). For instance, Newbill (2019) mentioned that although the EU created minimum CIP standards, it applies if a system disruption would affect two or more Member States. Therefore, each Member State is responsible for its CI and protective and defensive measures.

The Public-Private Partnerships (PPP) approach is a form of cooperation between the state and the private sector. Governments seek to achieve the benefits of PPP in public policies by utilizing digital infrastructures efficiently. Medaglia et al. (2017) stated benefits, such as risk sharing, service quality improvement, improved technological innovation, and cost reduction.

PPP is one of the useful, inevitable, and preferred ways of cooperation in CIP (Cavelty & Suter, 2009). The researchers clarified that public-private collaborative joint efforts through joint risk management in CIP contribute to security. Therefore, PPP benefits the goal of CIP by providing an opportunity to enhance security by more proficient risk mitigation in addition to efficient project management and enhanced technological innovation (Grasman et al., 2008).

In practice, the Estonian case represents the cooperation between the public and private sectors. Therefore, in this research, the PPP approach has been chosen to assess eID as a part of the CI to determine the benefits and impact of cooperation concerning CIP.

4 Research methodology

This chapter explains and justifies the research design and methodological approach. The following methodology has been identified and applied for this project to achieve the proposed aim of the research by answering the research questions.

4.1 Strategy

To assess the eID ecosystem as a part of the critical infrastructure, the case study strategy based on a deductive approach with the flexible design study process has been chosen for this thesis as the leading methodology. According to Yin (2009), the case study approach investigates contemporary or modern phenomena, events, situations, or organizations within a real-life context, where the researcher has little control over the event focusing on the real-life context. The case study strategy with the single case applies to the proposed research. It aims to explore the detailed real-life research case of the Estonian eID ecosystem, where the flexible design for the case study allows to consider which data is available and feasible to collect to make further analysis based on gained knowledge and understanding (Runeson et al., 2012).

The research topic includes different interconnected elements of the eID ecosystem and various critical infrastructure components, which is typical for a case study to contain many variables (Harrison et al., 2017). The deductive approach allows starting with the existing theories in the field of CI, which allows making final observations by researching the eID ecosystem based on the hypothesis (Runeson et al., 2012). A case study is a qualitative approach, in which a case or cases are discovered through detailed and in-depth data collection involving multiple sources of information, such as interviews, documents, reports, and observations, to present a case description and case-based themes (Creswell & Poth, 2016). Thus, the case study strategy for this research paper is applied to approach the complexity, which allows focusing on developing an in-depth description and case analysis by using multiple sources of evidence.

It is significant to consider that each research method is unique and different, which is also distinguished by the type of research question within the study. According to Yin (2009), the research questions in the case study research strategy generally start from “How” or “Why”. Therefore, the case study explains, describes, or explores phenomena

in everyday contexts. In this research, an explanatory structure has been applied based on the nature of the chosen case study.

4.2 Data collection methods

For this research project, qualitative data collection techniques have been used as a more common technique of collecting the data in the case study strategy (Crowe et al., 2011). This research required a complex and detailed understanding of the phenomena. According to Creswell et al. (2016), having considered the specification of qualitative research characteristics, the author of this research focused on multiple sources of evidence, both secondary and primary sources data.

For the secondary data collection method, academic writings, legal acts, open scientific sources, blogs and documentation provided valuable input for a case analysis by creating the theoretical background and the case description. The role of the theoretical framework is to contribute knowledge and justify the research by distinguishing areas through secondary sources (Runeson et al., 2012).

The author has chosen direct semi-structured expert interviews for the primary data collection method. Data collection through interviews is beneficial in receiving unique knowledge, which cannot be found in other data sources. A semi-structured type gives an advantage of flexibility, such as free question order and possible improvisation that allows deep investigation of how individuals experience the phenomena (Runeson et al., 2012).

The interview participants were selected based on the research strategy and research questions. Primary data was gathered from the key experts, who are concerned with different roles as the Estonian eID stakeholders from both public and private sectors, and also had been involved in the decision-making process of making eID a part of the state`s CI. Considering the qualitative nature, the main focus was to choose experts with different roles rather than replicate similarities (Runeson et al., 2012). Also, the Estonian case description showed the uniqueness of the public-private collaboration. Therefore, the target group of the interviews was focused on 6 experts from both: 3 experts from the public sector and 3 experts from the private sector. An overview of the interview participants is presented in Table 1.

Table 1. List of the interviewees.

Sector	Organization name	Role	Duration
Public	Health and Welfare Information Systems Centre (TEHIK)	Head of TEHIK	00:38
Public	Estonian Information System Authority (RIA)	eID Business Architect	01:10
Public	Estonian Police and Border Guard Board (PBGB)	Adviser-expert	00:42
Private	SK ID Solutions AS	CEO	00:43
Private	Cybernetica AS	Head of Digital Identity Technologies Department	00:42
Private	KPMG Baltics OÜ	Lead Auditor	00:47

Approximately one-hour interviews long were carried out in English and recorded for further transcript analysis. In the interview questions, the author used the term eID, which stated digital identification and digital signing based on the Estonian Emergency Act (Riigikogu, 2017).

The interview started with the introductory questions about the expert's background, followed by three main parts. The first part of the "Historical background" focused on eID becoming a part of the Estonian state`s CI. The second part of the "eID As-Is" explored the current situation of eID in Estonia. The last part of the "Further development" focused on exploring the expert`s general opinion of making eID a part of the CI. An overview of the interview questions is presented in Appendix 1.

4.3 Data analysis

In the qualitative data collection method, text plays a fundamental and crucial role in result interpretation. This research focused on analysing data in a written report format by examining the data collected through the interviews by capturing important information concerning the research questions. Therefore, thematic analysis was adopted to effectively perform valuable data analysis for qualitative research by going through the qualitative dataset. Thematic analysis organizes and presents the collected non-numerical data set in rich detail based on flexibility considering a large body of data (Braun & Clarke, 2006).

The thematic analysis aims to identify, analyze, and report themes within data. In this research, six phases of thematic analysis were followed as a basic guideline presented by Braun and Clarke (2006):

In the first phase, the author got familiarized with the collected data. The verbal data, namely semi-structured interviews, must be transcribed into the written format in this phase to conduct the thematic analysis. During the transcription, the first initial coding ideas are already identified. However, the transcript and interview recording should be checked for accuracy.

Having familiarized and transcribed the data, in the second phase, the author started the production of the initial codes across the entire data set by identifying the main features of the data. This phase aimed to organize the data into meaningful groups concerning the research questions. Considering the number of interviews, the author decided to code transcribed data manually by classifying and arranging information in tables to examine relationships in the data.

Having identified codes across the data set, phase three involves generating initial themes in the data by analyzing and combining the codes into the potential themes, which forms the basis of the thematic analysis. In this phase, the main themes introduce the initial thematic map. The author decided to utilize a widely used qualitative tool for data analysis, NVivo, to show the thematic map and related codes. NVivo is one of the helpful tools which helps manage, shape, analyze, and efficiently locate qualitative data (Creswell et al., 2016). This phase aimed to compare, analyze, and relate the context behind and across the codes.

The purpose of phase four is to review the themes to make the analysis more efficient by applying the final changes in the themes if needed. This process involves re-evaluating the thematic map by reviewing and refining the themes. This process ensures whether the author's identified themes are appropriate and sufficient for the research objectives.

The fifth phase focuses on naming and defining the themes. It is one of the crucial parts of the thematic analysis since it enables the author to set boundaries and distinguish between the data. During this phase, the specifics of each theme were refined. As a result, the themes, which will be presented in the analysis part, are clearly defined.

Last but not least, the final phase six represents the final writing part by producing the formal report of the findings. The author presented a vivid story within and across the themes with a discussion considering the research questions.

To increase the validity of the research within the case study, data triangulation is considered one of the significant and often applied approaches, including using data from different sources (Runeson et al., 2012). In this research, a theoretical framework identifies the possible components of the CI, which are applied to the Estonian case study context. The direct semi-structured expert interviews strengthen understanding and increase the validity of the research.

5 Case overview

Before assessing and analysing the eID ecosystem as a part of the critical infrastructure, it is significant to provide a current overview of the Estonian eID ecosystem and critical infrastructure in the Estonian context to understand how the entire system works. In this section, the 2017 ROCA case in Estonia shows the significance of the eID. It describes lessons learned based on the key implications of a security vulnerability in the Estonian eID system.

5.1 Estonian eID ecosystem

The digital identity system of Estonia, introduced in 2002, is called e-Estonia. Electronic identity and its ecosystem have already become a part of the citizens` daily transactions in public and private sectors (e-Estonia, n.d.). According to the e-Estonia facts and figures, 99% of Estonians have an ID card, which enables them to use eID, where 70% actively use digital ID cards, 17% have Mobile-ID, and 40% of Estonians use Smart-ID to access 99% of all government public e-services. As of 2021, over 98 million documents have been already signed with digital signatures. Also, by 2025 Estonia aims to provide a business environment and e-services for 10 million e-residents.

eID ecosystem is a complex system, including, for instance, ID cards and their production and issuance, user software, and services provided both by public and private companies (Veldre, 2017). In Estonia, the government has been identified both as the regulator to provide guidance, regulations, with management control of digital identities and as the unique identity provider to issue ID cards facilitating e-services (Pedroli et al., 2021).

According to the Republic of Estonia Information System Authority (RIA) (2021), eID is a collection of data that aims to connect a person with an electronic environment by applying a physical person identity to an electronic identity in Estonia. Under the Identity Document Act (Riigikogu, 2020), Estonian citizens and aliens residing in Estonia must hold an identity document issued by a state authority. The nationally issued official document is, in turn, the basis of the Estonian eID scheme (Police and Border Guard Board, 2018).

In Estonia, electronic identity is a government-driven centralized system with interoperable solutions launched with the participation of the private sector, which provides multiple credentials and authentication methods operating based on Public Key Infrastructure (PKI) solutions (Figure 5). The model is based on two cryptographic keys with corresponding certificates: public and private, allowing safe entry into e-services, namely digital authentication, giving digital signatures, and secure data transfer (Estonia Information System Authority [RIA], 2021).

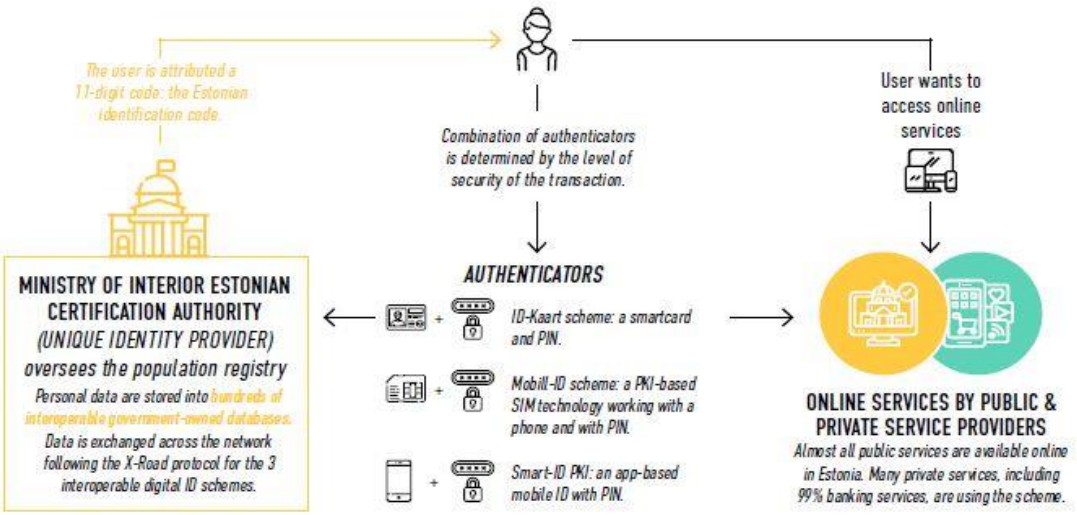

Figure 5. Estonian eID ecosystem (The Security Identity Alliance, 2021).

5.1.1 Estonian eID stakeholders

According to Lips et al. (2018), the Estonian eID ecosystem consists of different players and roles. It creates a unique and well-operating network necessary for the functioning of eID, where the Estonian Police and Border Guard Board (PBGB) and the Information System Authority (RIA) are the leading authorities, together with other partners from the public and private sectors.

RIA operates within the administrative area of the Ministry of Economic Affairs and Communications, which, in turn, is responsible for the eID policy and strategy to ensure the security and functioning of interoperable solutions with technological development (Ministry of Economic Affairs and Communications, 2018). RIA is the eID technical competence centre responsible for the development, quality, safety, and functioning of

the eID and PKI system, including cybersecurity incident management and trust service supervision (RIA, 2021).

PBGB is an eID scheme stakeholder that operates within the administrative area of the Ministry of the Interior, which is the second ministry responsible for the eID policy and strategy to ensure public safety and national security in the field of identity management (RIA, 2021). The authority is responsible for issuing identity documents and keeping up the eID scheme together with security partners, which manufacture and provide trust services. For instance, SK ID Solutions AS is a private company that is a subcontractor of identity documents qualified trust services of the PBGB, which issues the certificates and validity information of the eID certificates to use personalized e-services and give digital signatures.

In addition, the Estonian government agency of IT and development centre (SMIT) under the Ministry of Interior is responsible for offering different ICT services, such as technical support and the development of information systems in the internal security area. Also, the Ministry of Foreign Affairs is responsible for identity document management in embassies and the issuance of diplomatic IDs, including eIDs (RIA, 2021).

5.1.2 Estonian eID tokens

In Estonia, eID tokens enable electronic authentication and qualified electronic signatures, which is compliant with the eIDAS (electronic IDentification, Authentication and Trust Services) regulation adopted by the Council of the European Union (EU) and the European Parliament (RIA, 2021). The regulation aims to create an equal level of trust in both the digital and physical worlds. In Estonia, a digital signature corresponds to the highest level of trust. Also, in Estonia, assurance requirements come from European legislation, such as GDPR (General Data Protection Regulation) and national legislation, such as the Emergency Act and the Act of the Electronic Identification and Trust Services for Electronic Transactions, followed by both public and private parties (Eichholtzer, 2020).

In Estonia, there are six types of eIDs. In addition to a mandatory identity document (ID card), the Estonian eID ecosystem brings multiple tokens available with the same electronic functionalities issued by public or private sectors with a high level of assurance (Pedroli et al., 202). For instance, digital identity card (Digi-ID), e-Residency digital

identity card, residence permit card, diplomatic identity card, and ID card are smart card-based solutions. Also, there is a Mobile-ID solution, where the chip with eID functionality with the secure model is embedded in the SIM card that can be obtained from the Estonian mobile operators by having either an ID card or residence permit card as prerequisites (Eichholtzer, 2020). In addition, a certified Smart-ID solution is offered for authentication and signing purposes by the private entity of the trust service provider based on public-private cooperation.

5.2 Critical infrastructure in Estonia

According to the Council of the EU (2008), Estonia defines critical infrastructure as a system or asset which is vital to maintain social functioning, such as health, security, safety, economic and social well-being, the disruption of which would have an impact as a result of failure those functions. Also, maintenance reliability and safety of information and communication systems is an essential part of the CI for the country's functioning, which defines critical information infrastructure (CII).

In Estonia, critical information infrastructure protection (CIIP) aims to maintain the functioning of essential information and communication systems on a national level for a public and private network, in which RIA serves as a Supervisory Body (RIA, 2021). Activities of CIIP seek to increase cyber security awareness and development of security measures implementation by giving a recommendation of risk analysis to service providers. Protection is regulated by providing the regulation of risk assessment requirements, including a description of security measures.

Estonian cyber security strategy is also a part of the CIIP (RIA, 2021). One of the purposes of cyber security development is critical infrastructure and vital services areas. Estonian Ministry of Economic Affairs and Communications (2020) stated that the security of information systems used to provide critical and vital services is crucial for the functioning of economic and social welfare. Therefore, the Estonian cyber security strategy focuses on resilience to sustain a digital society by relying on cryptographic solutions, transparency, and public trust, which is the foundation of the Estonian digital ecosystem.

According to the Estonian Digital Society 2030 Development Plan (Ministry of Economic Affairs and Communications, 2021), Estonia aims to develop a successful digital society where cyber security plays a significant role in ensuring high-quality public services by guaranteeing people`s fundamental rights. Collaboration of the key partners from both public and private sectors gives the economy a competitive advantage and the best digital experience by creating a long-term digital strategy.

5.3 The ROCA case

In 2017, Estonia became a case of critical security vulnerability, which is internationally known as the ROCA (Return of the Coppersmith Attack) cryptographic vulnerability discovered in 2017. In addition to several EU countries, Estonia also has been notified of the potential security vulnerability in the Estonian state-provided ID card chips issued since Autumn 2014. Coppersmith`s algorithm is mainly used in scenarios where partial information of a private key or message may allow to compute the rest of the information (May, as cited in Nemec et al., 2017). As a result, the private key used for authentication and signing could be calculated from the public key. Consequently, it could make possible authentication, decryption, and document signing without a physical card possession, which required immediate action by the state (RIA, 2018).

The 2017 ROCA case in Estonia became exceptional. Due to the significant dependency and demand on eID from the state`s perspective and the end-users for both individuals and businesses provided a large-scale security issue. Valtna-Dvořák et al. (2021) analyzed the implication of the ROCA case presented on the Estonian eID mechanism by focusing on eID and crisis management aspects, which aimed to propose lessons learned for further policy recommendations. The research proposed that the state is responsible for guaranteeing the security of the eID, which includes identifying the roles of the stakeholders, eID security provision, continuous political management, and guiding operational with crisis management.

Also, having handled the ROCA vulnerability, the case showed the inevitable impact of the public-private partnership in the Estonian eID scheme. Although the private sector interests influence the state, however, PPP demonstrated mutual engagement in crisis management by sharing common values (Valtna-Dvořák et al., 2021). Also, Lips et al. (2018) proposed that although Estonia is a relatively small country, however, PPP is one

of the key contributing factors in solving the Estonian eID crisis in addition to agile management, technological advancement, openness, and performance analysis.

In addition to the PPP factor, Lips et al. (2018) stated that alternative eID tokens and available alternative renewal certification services played a crucial role as a technical success factor in handling with eID crisis. Although the public sector is considered more conservative and slower to change, however, the research showed that, in crisis management, Estonia demonstrated fast implemented approaches, which benefited from agile project-based management and single authority coordination. Also, Estonia succeeded in fast verification of new technical solutions by having a technical lawyer adviser in the early stage to prevent further security weaknesses and mistakes (Lips et al., 2018).

The 2017 ROCA case demonstrated the responsibility and importance of the Estonian state towards the potential negative impact on the daily functioning of society, which also revealed challenges in terms of regulations between the state and the EU. Therefore, a comparison of the eIDAS emerging practice regulation and interpretation was required (Valtna-Dvořák et al., 2021).

In Estonia, some public services are primarily in the electronic version, which demonstrate dependency on the state`s digital ecosystem. Thus, Estonian eID is recognized as one of the key enabling elements. According to the Emergency Act (Riigikogu, 2017), digital signing and digital identification are presented in the list of vital services, the continuity of which should be organized by the RIA in case of an emergency. Therefore, since 2017, digital signing and authentication in Estonia have been considered part of the state's critical infrastructure.

The 2017 ROCA case in Estonia became valuable in developing the eID system based on further improvement of the environment and process to cope with possible vulnerability issues. Valtna-Dvořák et al. (2021) stated that the Estonian case could provide input for the other countries as the latest development of the eID system. Having analyzed the global and Estonian impact of the 2017 ROCA case, RIA (2018) provided the following four recommendations:

- Information sharing and vulnerability disclosure: To reassess the international notification mechanism and consider international risk and vulnerability joint sharing.
- Risk management and continuity planning: To develop and integrate electronic alternatives to ID cards and several crypto libraries.
- Role of governments in introducing innovation: Despite competencies, which lie in the private sector, governments should influence in developing, procuring, and certifying technology.
- Openness: To involve broad-based cooperation between national, international, and corporate stakeholders for long-term solutions.

In addition to mentioned recommendations, Parsovs (2020) studied the legal and technical issues that appeared while resolving the vulnerability eID crisis in Estonia. The research stated that such causes as the lack of technical preparedness, making decisions under time pressure, and critical situations are challenging legal requirements, which may result in legal non-compliances. The researcher stated the importance of updating the legal framework to ensure legal certainty for the ecosystem participants.

6 Research results and findings

The thematic analysis was used to analyze the qualitative data to answer the main research question and its sub-questions. It allows highlighting the codes, which will correspond to research objectives by creating the themes. Interview questions were divided into three parts. These parts aimed to identify the process of the Estonian case of eID becoming a part of the state`s CI, the critical eID components considering criticality factors and resilience in the concept of CI, and the state of eID being a part of the state`s CI by looking its requirements and preconditions. Each part represents a thematic map.

6.1 Estonian case background

As a result of the first part of the findings, interviewees` opinions divided on whether eID became a part of the critical infrastructure in Estonia on time. The overall process and implementation could take less time to mitigate the vulnerability. However, the whole process is complicated and takes time due to its uniqueness and difference from other vital services.

The interviewees` opinions were divided based on different influential conditions and prerequisites that forced and showed the readiness of eID to become a part of the CI. Figure 6 shows the Estonian background of how eID became a part of the CI supported by the forced conditions and prerequisites that showed the readiness of eID to become a state`s CI summarized by themes such as cooperation, critical dependence, necessity, and government.

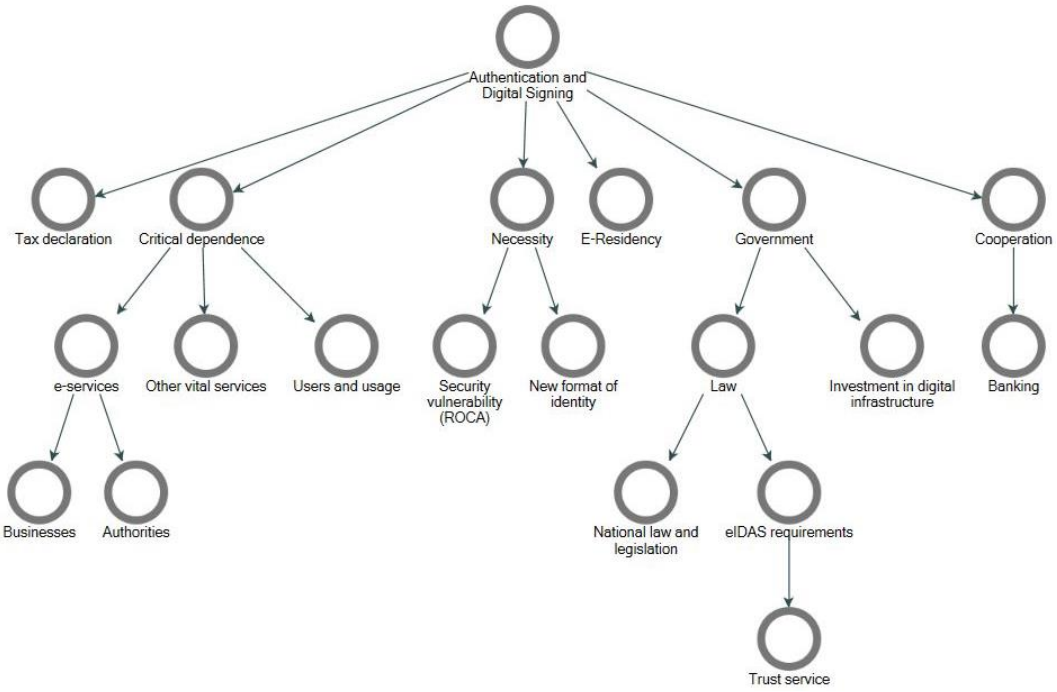

Figure 6. Estonian case overview.

According to the interviewees, eID became a part of the state`s CI from the government perspective in Estonia, which was regulated by law. The main decision was supported by different factors, such as electronic signatures, which became equal to paper signing, and integrated authentication options into the government systems.

The interviewee mentioned that the journey started with implementing a new identity document (ID card) format that was integrated into the electronic environment and became vital in terms of usage. Critical dependence played a crucial role justified by many new e-services on the market used by authorities and businesses, supported by other daily dependent vital services. These dependencies required the highest and most secured authentication and digital signing level. In 2017, the ROCA case justified the necessity and became one of the driving forces to include eID in the Emergency Act.

Also, the interviewee stated that one of the strongest forcing conditions was banking, namely online banking, which requires the most secure authentication solution. Cooperation with the bank sector became crucial. The interviewee identified the bank as a key element, indicating that eID should be a part of the CI. Also, additional unique drivers, such as online tax declaration and e-residency, were mentioned.

The interviewees were asked to provide critical changes since eID became a part of the CI and the most challenging parts of the implementation process (Table 2). Some processes have been changed, added, edited, and regulated from the vital service perspective. Having considered experience in the eID field, challenges also became more precise.

Table 2. Changes and critical challenges of the case.

Changes	**Challenges**
Implementation of critical information security requirements	Government and law
Audits	IT systems, including eID software
Business continuity plan	Security requirements and risk management
Risk management documentation based on the law requirements	Validation services and certificates
Additional regulations at the national level	Realizing the scope of the service
Updating Cyber security and Emergency Act	To build service level
	Cooperation between different expert groups

Interviewees mentioned that eIDAS regulation played a significant role in creating eID regulatory requirements and provision of trust service. However, additional national regulation was required for the trust service provider also considering digital identification as a part of vital service, which also required changes in audits to maintain service continuity and sustainability.

Vital services require better risk assessment and risk mitigation. The interviewee mentioned that Estonia had had risk management in place that did not change much, but additional critical information security requirements with the business continuity plan were implemented, and risk management was legalized to mitigate critical situations and risks.

However, risk management received special attention from a challenging perspective to get security requirements, due to the difficulty of predicting and mitigating all the risks. In addition, risk management is supported by other continuous challenges, such as understanding the scope of the vital service, due to its dependency on different elements, for instance, the Internet provider, eID software, time-stamping service, certificates, and supporting IT systems.

Therefore, the challenging part starts with the government and law to regulate the process applicable to all parties. The interviewee stated that there had been many discussions to determine, which parts of eID should be part of the CI since each part of the ecosystem should be a part of it.

In addition, the interviewee also supported the challenge from the organizational perspective to achieve understanding and cooperation between different expert groups. Also, the interviewee summarized that the challenge of this process lies in the implementation of required changes.

6.2 Critical eID ecosystem elements

As a result of the second part of the interview, the interviewees agreed that eID is a comprehensive ecosystem with many interconnected critical elements. Interviewees stated that failure of one component might affect all criticality characteristics, such as proportion, time, and quality. However, the interviewee stated its uniqueness. For example, the interviewee noted that the ID chip malfunction is characterized by proportion and time, although the malfunction of different eID tokens may affect the quality of service delivery. Also, the trust service provider has been assessed as proportion, the certificates of which belong to the time and quality characteristics (Table 3). Moreover, the interviewee considered proportion, time, and quality characteristics as

separate critical components. The interviewee stated that time and quality components are significant in providing trust in the eID solutions.

Table 3. eID ecosystem elements.

Proportion	**Time**	**Quality**
ID chip	ID chip	eID tokens
Trust service provider	Validation service	Service quality, certificates

To identify critical components in addition to assessing criticality characteristics, the elements were selected based on the resilience concept, which is viewed in the CI context as a quality reducing vulnerability affected by disruptive factors by presenting preparedness for the emergencies. Interviewees explained and gave examples of eID ecosystem critical components from technical and organizational perspectives.

Figure 7 represents the eID ecosystem's critical elements, the failure of which may significantly impact the vital functions of society summarized by technical and organizational themes.

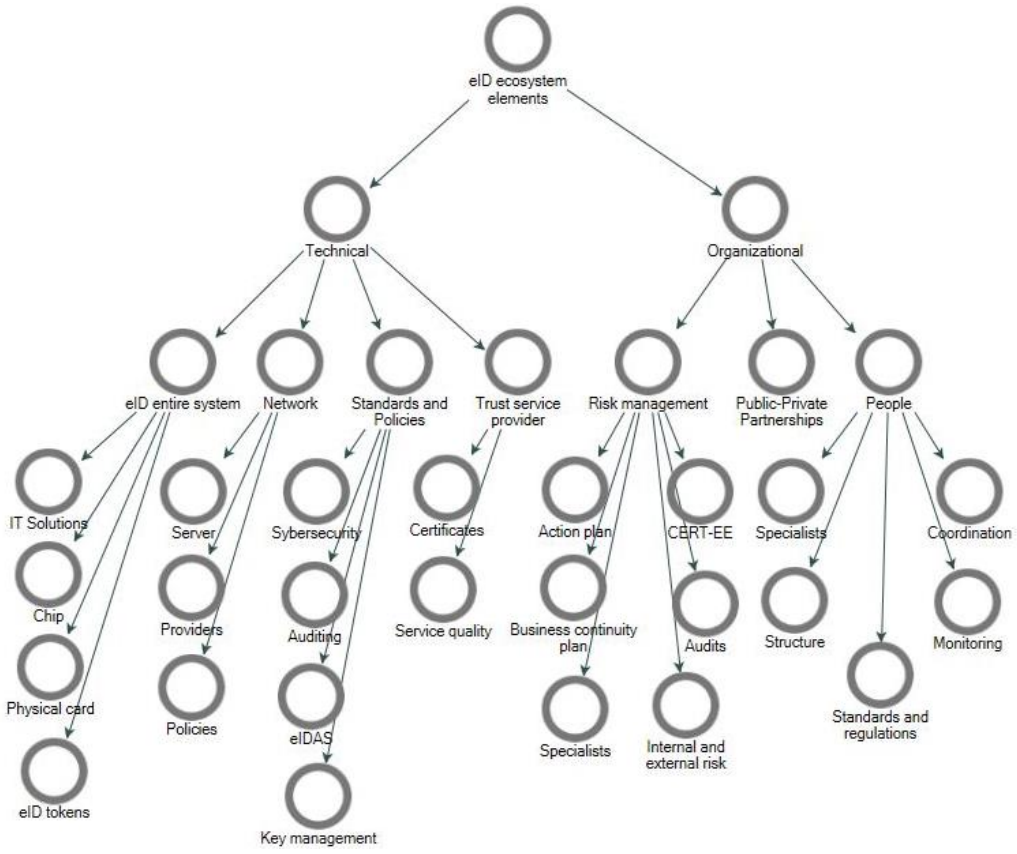

Figure 7. eID ecosystem critical elements.

Technical components required special attention due to the eID ecosystem's uniqueness. Interviewees agreed that eID should be considered a whole eID entire system consisting of different critical elements behind the digital identification and signing processes. The interviewee said that from the legal perspective, the government has decided to issue different eID tokens, which, as a result, has strengthened the resilience system.

The network received special comments and required special attention from the vital service perspective directly impacting eID solutions. The interviewee stated that network failure would significantly impact society, which will provide additional vulnerability to other dependent vital service provisions. The interviewee noted that the issue with the network in Estonia might provide high-level damage in terms of the eID solutions.

In the eID ecosystem, cyber-attacks are considered a significant threat and other security vulnerabilities are top priorities. Therefore, standards and policies should be verified, monitored, and audited according to the legislation. The interviewee mentioned that security and monitoring procedures should be applied to information systems regularly according to standardized procedures and documentation.

From the technical perspective, the trust service provider is responsible for providing authentication and digital signing certificates. eID solutions are very dependent on the trust service provider, which requires special regulations, maintenance, and auditing for service quality and organisation. The interviewee stated that the eIDAS regulation provided direct standards for assessing fundamental security and resilience of trust services, making it easier for the government side to rely on making audits on this standard.

The interview results present risk management as an embedded part of the organizational procedures, dependent on communication and relationship strategy between involved parties. Interviewees stated that all risks could not be predicted, but the process of how to start solving the risks must be written down and agreed upon by responsible parties, in which RIA play a key role, in Estonia, supported by CERT national contact point to handle incidents. Although the risks should be mapped, assessed, and measured, it should be a living process, which should be done regularly considering the whole system. In Estonia, the government is doing its risk management, but there are also requirements for the service provider, which are audited. Also, backup solutions should be in place to mitigate the risks in case of failure.

The public-Private Partnerships element has been mentioned from the organizational side, which makes valuable cooperation by identifying its crucial role. The PPP is a huge, trustworthy, and close partnership in Estonia, where the government shares critical parts of the eID ecosystem with the private sector. The interviewee mentioned that if the public sector has tendered some of the services from the private sector, there is an advantage of knowledge sharing and better control over the technical components, which strengthens the ecosystem. The interviewee mentioned an advantage of such collaboration of making more trust in society, justifying that government does not own and provide everything by itself. Such cooperation is also very crucial for managing the risks.

As a result of interviews, people are an essential element of the eID ecosystem from the organizational side for the ecosystem. Interviewees agreed that bad and poorly audited internal policies and requirements might provide potential damage. The interviewee added that clear tasks and responsibilities must be coordinated between and inside the organization to prevent vulnerability to disruptive events by supporting different organizational structures with the same capabilities.

6.3 eID Ecosystem design

As a result of the third part of the interview, the interviewees provided different opinions on whether the eID ecosystem should be a part of the state CI, supported by advantages and disadvantages (Table 4).

Table 4. Advantages and disadvantages of eID being a part of CI.

Advantages	Disadvantages
Service providers better understand their roles	Management pressure
Government can regulate the process better	More laws and regulations to track
Society can rely on service	Bureaucracy
Better risk management	Legal issues from the government side
Better quality and assurance for dependent services and vital services	More damage if regulated poorly
	More resources and expences

Making the eID ecosystem a part of the state`s CI is dependent on its key influential elements, which show that eID should be a part of the CI and preconditions that need to be fulfilled by the country before making eID a part of it. Figure 8 represents the design of the eID ecosystem by showing the themes of summarising the key influential elements and necessary preconditions.

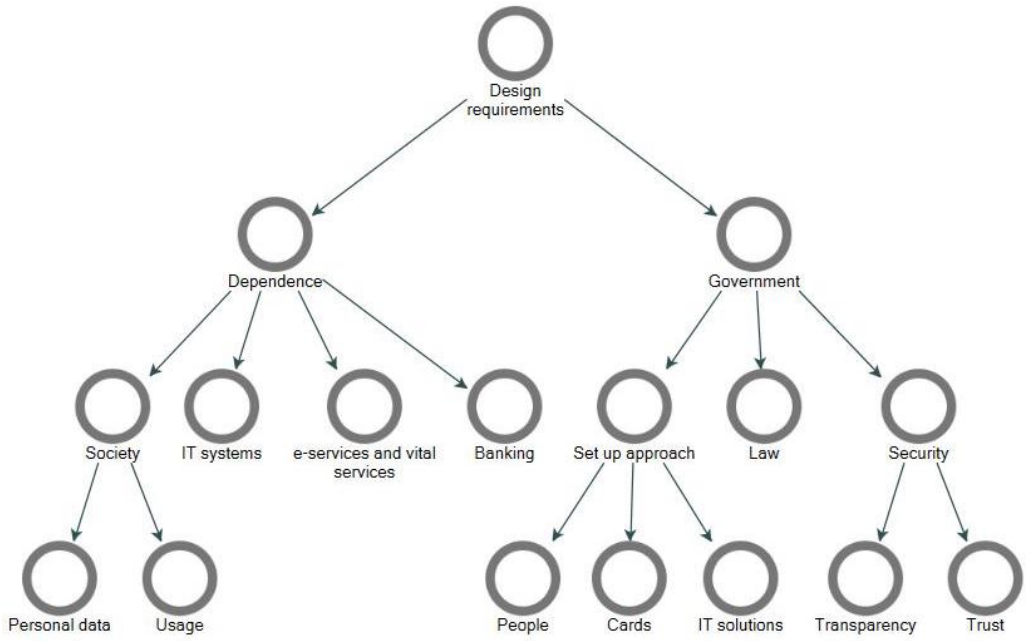

Figure 8. eID ecosystem as a part of the CI.

To identify whether the eID ecosystem should be a part of the CI, it is significant to start by assessing its impact on society. The interviewees agreed on assessing the dependency on eID solutions, which indicates the necessity of making eID a part of the CI. For instance, the interviewee stated that it depends on other connected vital services and IT systems dependent on eID solutions used by other interested parties, stakeholders, and authorities. Therefore, from the governmental side, it becomes critical to think about personal data and information preservation, which belong to the government and do not belong to the private entities. Also, the interviewee mentioned that cooperation with the financial sector, namely banks, is a critical element in identifying the necessity of making eID a part of the CI based on usage and essential security requirements.

The interviewee stated that each country's case could be different by clarifying that vital services and the integration process into vital services are national-dependent, and the country should know what is critical. To begin with, the interviewee stated that the government should start with the legal binding from the law side. Also, it is significant to identify an approach to set up the eID system and the digital signing, which will be supported by the required experts in the field and available IT solutions on the market. The interviewee added that the government should think about security and how to achieve transparency and trust in security.

7 Discussion

In this thesis, having researched the Estonian case, the phenomenon of the eID ecosystem being a part of the state`s critical infrastructure has been assessed. This chapter presents the answer to the main research question, which aims to provide an explanatory solution of how it is possible to identify that the eID ecosystem is ready to be a part of the state`s critical infrastructure.

This research aims to promote the development of a secure, trustworthy, sustainable, and data-privacy centric eID by assessing the eID ecosystem as a part of the state`s critical infrastructure. This thesis seeks to apply the main critical infrastructure principles to the eID concept to strengthen the resilience of the eID solutions by identifying the eID critical components supported by designed requirements and necessary preconditions based on the Estonian case. As a result, this research might strengthen digitalization and support the e-governance strategy by focusing on the security and protection of digital identification in developed and developing countries.

This chapter also gives recommendations for implementation and acknowledges the research limitations.

Defining critical infrastructure

According to the findings from the previous literature, critical infrastructure has been identified as a complex system, which consists of visible and invisible components. Although the term CI states to the structure that humans utilize to provide vital social goods or services, however, at the global level, the concept of CI does not have clear boundaries of what constitutes CI. Therefore, CI has been studied by approaching the designation of CI elements to understand what is critical to achieving better infrastructure resilience to facilitate CIP.

According to the secondary research findings, the definition of CI has been changed in different nation-states due to the variations of criticality criteria, which creates concerns in defining CI at the global or rigorous level. Therefore, according to the theoretical framework, each nation-state should determine which services, goods or assets are critical and significant for society, the disruption or failure of which may significantly impact society`s well-being, economy, or state interest.

Estonian eID is a unique solution. Since 2017, in Estonia, eID, namely digital identification and digital signing, have been considered vital services and, on a legal basis, have been included in the Emergency Act, which is used for crisis management to ensure the continuity of vital services by preparing and resolving emergencies. Thus, it can be stated that, in Estonia, eID is essential for the maintenance of societal functions, the disruption or destruction of which would have a significant impact as a result of the failure to maintain societal functions.

Estonia has had a long journey, which includes critical changes and challenges supported by various critical factors to achieve on the legal basis eID vital significance.

Design requirements and preconditions

To begin with, it is significant for the government to start by identifying whether eID became critical for society by assessing the eID requirements based on the key elements, which provide critical indicators. Having studied the Estonian case, the thematic analysis identified critical requirements by analyzing special conditions that forced to include eID as a part of the CI and prerequisites, which showed the readiness of eID to become a part of the CI.

Along with the theory, criticality assessment is the assessment of risks, which may provide a significant impact in case of element failure. In Estonia, eID has been recognized as one of the key enabling elements in the state`s digital ecosystem, which was regulated by law due to the high-security assurance requirements influenced by the value of the digital signature and the amount of personal data owned by the government.

The Estonian case showed that elements that indicate the dependency on eID for society should be assessed to understand eID criticality. For instance, such dependent services or e-services have many users and are integrated into the government system and responsible for health, safety, security, economic, or social well-being. The 2017 ROCA case crisis justified the eID dependency from the state`s perspective and the end-users, which became one element that indicates the necessity of eID to become more secure.

Also, the research findings show that one of the key enablers of the eID criticality is cooperation with banks, which requires secure authentication methods for online banking. However, the collaboration between the government and banks becomes valuable if both

sides seek an integrated and secure identification solution. Banks play a significant role in terms of the number of users and service usage frequency.

Along with the critical requirements, which indicate the eID criticality for society, the findings also showed the preconditions, which must be considered as a part of the eID criticality foundation, where the government has been identified as a key operating centre.

The thematic analysis identified critical preconditions, which constitute the eID ecosystem's critical requirements. Along with the theory of CI complexity, the eID has justified its complication, which requires considering eID as an entire system, including cyber security strategy as a part of a digital development plan and the whole eID set-up approach supported by the law of the national identity document.

Also, considering the EU requirements, eIDAS regulation requires a qualified trust service provider to provide qualified certificates to electronic signatures, which should be considered as a part of the eID ecosystem. The significance of the trust service provider has been justified by the fact that a digital signature legally equals a handwritten signature.

It might be stated that eID should be seen as a whole ecosystem by considering all interconnected critical elements, which should be regulated on a legal basis and correspond to the equal value of vital services.

eID critical infrastructure components

In a concept of CI, resilience plays a significant role by presenting preparedness for emergencies to avoid a negative impact on a population or economy due to failure. Along with the theory, the thematic analysis has identified the eID ecosystem's critical elements, which reduce vulnerability by strengthening technical resilience and organizational resilience.

The findings proposed that technical resilience in the eID ecosystem can be achieved by considering the whole eID entire system. The government plays a crucial role by supporting and providing the standards and policies to ensure certainty for the ecosystem participants and procedures, which should be audited. Particularly, in the Estonian case and the European regulation, the provision of trust service requires regulation on the national level since a private entity provides trust service. In addition to the entire eID system, the findings show that integrating different alternative eID tokens played a crucial

role as a technical success factor during the crisis. In addition to the eID entire system, it is significant to focus on the network and its resilience. Since eID is highly dependent on network and information communication system provision and quality, maintaining and regulating information and communication systems on a national level for both public and private networks are essential.

According to the theoretical framework, organizational resilience aims to strengthen organizational resilience based on individual factors to adapt to changes, rather than assessing only technical resilience. The primary research findings identified risk management as a part of organizational resilience, which should be embedded into the organizational procedure to be mapped, assessed, and regularly measured. However, considering the Estonian case, the government should support internal and external risk management to support resilience. In addition to the Public-Private Partnerships, it is significant to support and coordinate specialists in the field based on the organisation's structure and regulations.

eID critical infrastructure protection

CIP is crucial to attempting a better and more secure CI by strengthening its resilience toward disruptive events. According to the secondary research, each nation is responsible for its CI protective and defensive measures, and therefore, CIP should be a part of national security.

The theory states that the approach of PPP provides significant benefits by utilizing a form of cooperation in the field of CIP between the state and the private sector, which, as a result, contributes to security and proficient risk mitigation due to risk sharing, service quality improvement, and technological innovations.

The primary research identified that PPP is an organizational element that strengthens the eID ecosystem's resilience through knowledge sharing and common values. The ROCA case demonstrated the inventible impact of the PPP in Estonia by mutual engagement in crisis management, which became one of the key contributing factors. Also, the findings show that mutual value sharing provides more trust and transparency for society since the public sector is considered more conservative and slower to change than the private sector.

Although Estonia is a relatively small country, however, PPP might also be risky in terms of the private sector interest changes, which might be influenced by profit or receive a negative impact from the legal side, where the government might lose control. Therefore, the government should balance value sharing and regulations to clarify roles and responsibilities to benefit from cooperation.

Outcomes

As a result of the discussion, figure 9 summarizes the main CI principles applied to assessing the eID ecosystem as a part of the state`s CI to achieve secure, trustworthy, and sustainable eID solutions. Each process includes the key elements identified within this research. Critical indicators, required preconditions, and resilience elements are presented in the explanatory checklist in Appendix 2, which is mentioned further in this chapter.

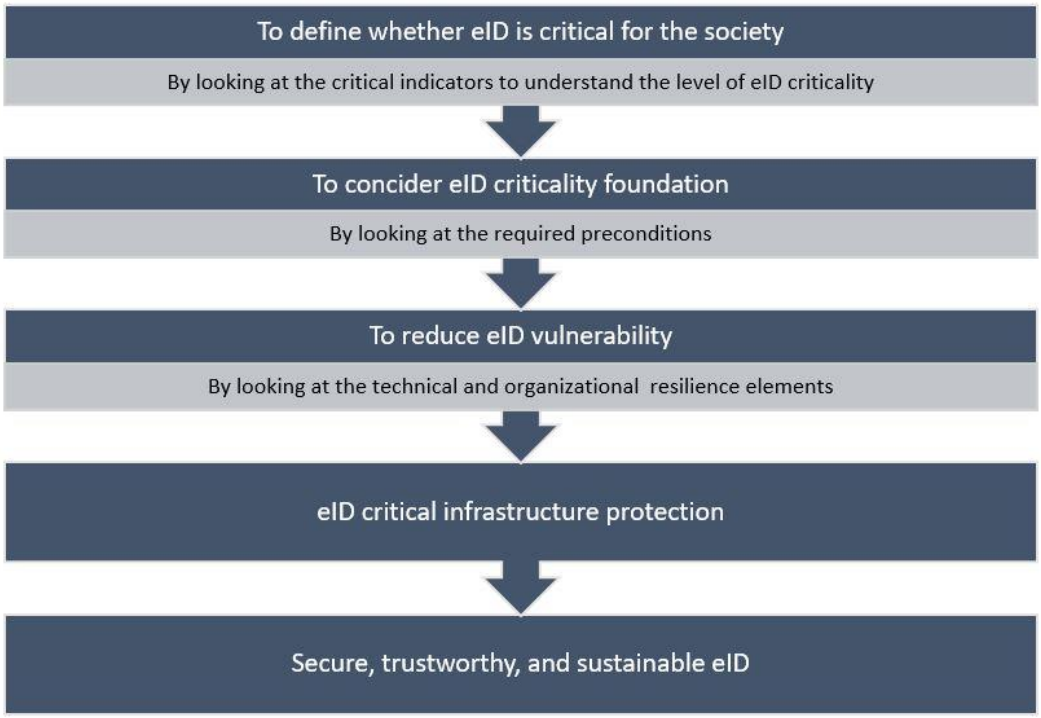

Figure 9.The process of assessing eID as a part of the state`s CI.

The concept of CI is significantly interconnected with the concept of resilience and protection. It gives a significant advantage by focusing on providing quality and security for the state`s critical assets or services.

Assessment of the eID ecosystem as part of the state`s CI brings significant advantages for the government to better regulate the process by improving risk management, which

provides better quality and assurance for dependent and vital services. Therefore, service providers will understand their roles, which may enhance society's reliability by focusing on identity privacy.

Considering digital transformation and technological development, the demand for a secure eID has increased and has become an essential part of e-governance. Assessing eID as a part of the CI on time may prevent serious damage to society's well-being, save resources, facilitate business continuity, and provide more ease access to e-services based on transparency.

eID as a CI is a government-driven comprehensive system with different interoperable elements. Having researched the Estonian case of how the eID ecosystem became a part of the state`s CI, the checklist of requirements and preconditions supported by the eID critical resilient elements is presented to facilitate CIP (Appendix 2).

As a result of the thesis, the checklist presents an explanatory tool for the government with identified eID critical elements to facilitate critical requirements of identifying eID criticality supported by a critical foundation to proceed with resilience elements and critical infrastructure protection. The purpose of the checklist is based on the gained knowledge to indicate the early signs of the eID critical necessity from the society to make government decisions towards successful eID vital significance and proceed with the secure and resilient eID solution.

7.1 Recommendations

Based on the research objectives and findings, the author provides the following recommendations for the government that are important to consider mitigating possible challenges in assessing and implementing the eID as a part of the state's critical infrastructure:

1. To provide single authority coordination responsible for eID policy, strategy to ensure the security, functioning of interoperable solutions, quality, safety, and technological development.

2. To understand the scope of the eID service and interdependent elements, which require special attention and changes to assure eID continuity.

3. To provide trust services on a national level to increase transparency and gain more control regulated by the national law.

4. Network and trust services should also be considered a part of the CI.

5. To establish a national point in IT security to manage security incidents.

6. To focus on support and motivation for experts from the public sector to avoid complete control by private sector experts.

8 Limitations and future research direction

The research of this thesis is limited by the specifics of a chosen case study. Estonia is a relatively small country. The specifics, such as the size of the country and population, are crucial for continuing with implementation. Also, Estonia is a member state of the EU, which has a partial legal impact that applies at the national level that is significant to consider.

This thesis provides the foundation to continue more detailed research on the resilience of the eID critical elements by conducting a qualitative criticality assessment from the technical or organizational perspective. Also, considering the specifics of a case study strategy, the approach of PPP can be investigated in application to different cases to facilitate CIP, such as countries with a different size of a population. Also, the impact of other CIP approaches in eID can be considered for future research.

In addition, future research can be done by implementing the achieved results of this thesis in different countries. Therefore, future implementation can provide a more detailed assessment by focusing on critical eID elements in the real-life context.

9 Summary

This research aimed to present the assessment of the eID and the ecosystem around it as part of the state's critical infrastructure by identifying the readiness of the eID and its ecosystem to become a vital service which facilitates the critical functioning of a society. As a result of researching the Estonian case, this thesis focused on secure, sustainable, and reliable eID solutions to encourage digital transformation by focusing on high-value e-services and efficient digital governance in developed and developing countries.

Qualitative data collection techniques and the case study methodology as the main methodology were used for this thesis. Along with the secondary sources, the primary data was collected from direct semi-structured interviews with Estonian experts from the eID field. This research adopted thematic analysis to perform qualitative data analysis to provide an explanatory solution.

During the research, the author investigated the concept of critical infrastructure by applying it to the eID field. Having considered that eID being a part of the state`s CI is a relatively new phenomenon, the author started the research by providing a general theoretical background to identify the concept of CI by focusing on the theories on critical elements, the concept of resilience, and the theory of critical infrastructure protection.

Having researched the Estonian case, the results showed the complexity and uniqueness of the eID ecosystem with many interconnected elements, which should be considered as an entire system. Along with the CI theories, this thesis has identified the critical eID elements, which facilitate critical requirements of determining the readiness and indicate the importance of eID vital significance supported by the critical foundation elements to proceed with the eID ecosystem resilience and critical infrastructure protection.

References

Al-Khouri, A. (2014). Digital identity: Transforming GCC economies. *Innovation (North Sydney)*, 16(2), 184-194.

Asgarkhani, M. (2005). Digital government and its effectiveness in public management reform: A local government perspective. *Public Management Review*, 7(3), 465-487.

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101.

Brunner, E. M., & Suter, M. (2008). *International CIIP handbook 2008/2009: An inventory of 25 national and 7 international critical information infrastructure protection policies*. Center for Security Studies (CSS), ETH Zürich.

Camp, L. (2003). Identity, authentication, and identifiers in digital government. *Proceedings. International Symposium on Technology and Society, 2003. Crime Prevention, Security and Design. 2003*, 10-13.

Council of the European Union. (2008). Council Directive 2008/114/EC. *Special edition in Croatian*, 18(003), 72 – 179.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology, 11*(1), 100.

Dunn-Cavelty, M., & Suter, M. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-187.

E-Estonia. (n.d.). *e-Identity.* E-Estonia. Retrieved March 4, 2022, from: https://e-estonia.com/solutions/e-identity/id-card/

E-Estonia. (n.d.). *Facts and Figures.* E-Estonia. Retrieved May 5, 2022, from: https://e-estonia.com/facts-and-figures/

E-Governance Academy. (2016). *e-Estonia - e-governance in practice*. eGA. Retrieved February 01, 2022, from: https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf

Eichholtzer, M. (2020). *Overview of pre-notified and notified eID schemes under eIDAS: Estonia.* Atlassian. Retrieved March 17, 2022, from: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia

Fekete, A. (2012). Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science,* 2(1), 15-24.

Grasman, S., Faulin, J., & Lera-Lopez, F. (2008). Public-Private Partnerships for technology growth in the public sector. *2008 IEEE International Engineering Management Conference,* 1-4.

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case study research: Foundations and methodological orientations. *Forum qualitative Sozialforschung/Forum: qualitative social research,*18 (1), 1-17.

Leitner, B., Môcová, L., & Hromada, M. (2017). A New Approach to Identification of Critical Elements in Railway Infrastructure. *Procedia Engineering, 187,* 143-149.

Lips, S., Aas, K., Pappel, I., & Draheim, D. (2019). Designing an Effective Long-Term Identity Management Strategy for a Mature e-State. *Electronic Government and the Information Systems Perspective,* 11709, 221-234.

Lips, S., Aas, K., Pappel, I., & Draheim, D. (2019). Designing an Effective Long-Term Identity Management Strategy for a Mature e-State. *Electronic Government and the Information Systems Perspective,* 11709, 221-234.

Lips, S., Pappel, I., Tsap, V., & Draheim, D. (2018). Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field. *Electronic Government and the Information Systems Perspective,* 60-70.

Masiero, S. (2020). COVID-19: What does it mean for digital social protection? *Big Data & Society, 7*(2), Big data & society, 2020-12, Vol.7 (2).

Medaglia, R., Hedman, J., & Eaton, B. (2017). Public-private collaboration in the emergence of a national electronic identification policy: The case of NemID in Denmark. *Hawaii International Conference on System Sciences*, 2782–2791.

Mir, U., Kar, A., Dwivedi, Y., Gupta, M., & Sharma, R. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. *Government Information Quarterly*, 37(2), 101442.

Morgan, D., & Parsovs, A. (2017). Using the Estonian Electronic Identity Card for Authentication to a Machine. *Secure IT Systems, 10674*, 175-191.

Nemec, M., Sys, M., Svenda, P., Klinec, D., & Matyas, V. (2017). The return of coppersmith's attack: Practical factorization of widely used RSA moduli. *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1631-1648.

Newbill, C. (2019). Defining Critical Infrastructure for a Global Application. *Indiana Journal of Global Legal Studies, 26*(2), 761-780.

Novotny, P., & Janosikova, M. (2020). Designating Regional Elements System in a Critical Infrastructure System in the Context of the Czech Republic. *Systems (Basel), 8*(2), 13.

OECD. (2019). *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies. OECD. Retrieved February 08, 2022, from: https://doi.org/10.1787/02f0e5a0-en

Parsovs, A. (2013). Practical issues with TLS client certificate authentication. *Cryptology ePrint Archive*.

Parsovs, A. (2020). Solving the Estonian ID card crisis: the legal issues. *In ISCRAM 2020 Conference Proceedings-17th International Conference on Information Systems for Crisis Response and Management*, 459-471.

Pedroli, P., O`Neill, G., Fravolini, A., & Marcon, L. (2021). *Overview of Member States' eID strategies.* European Commission. Retrieved March 5, 2022, from: https://ec.europa.eu/cefdigital/wiki/download/attachments/364643428/eID_Strategies_v4.0.pdf

Perez, L. (2021). *Witnesses on Digital Identity as a Critical Infrastructure.* Meritalk. Retrieved November 14, 2021, from: https://www.meritalk.com/articles/witnesses-on-digital-identity-as-a-critical-infrastructure/

Popescu, C., & Simion, C. (2012). A method for defining critical infrastructures. *Energy (Oxford)*, 42(1), 32-34.

Rasouli, H., Valmohammadi, C., Azad, N., & Abbaspour Esfeden, G. (2021). Proposing a digital identity management framework: A mixed-method approach. *Concurrency and Computation, 33*(17), N/a.

Rehak, D. (2020). Assessing and strengthening organisational resilience in a critical infrastructure system: Case study of the Slovak Republic. *Safety Science, 123*, 104573.

Rehak, D., Senovsky, P., & Slivkova, S. (2018). Resilience of critical infrastructure elements and its main factors. *Systems (Basel), 6*(2), 21.

Rehak, D., Senovsky, P., Hromada, M., & Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection, 25*, 125-138.

Republic of Estonia Information System Authority. (2018). *ROCA Vulnerability and eID: Lessons Learned.* RIA. Retrieved March 8, 2022, from: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html

Republic of Estonia Information System Authority. (2021). *Critical Information Infrastructure Protection CIIP*. Ria. Retrieved March 3, 2022, from:

https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html

Republic of Estonia Information System Authority. (2021). *Electronic Identity eID.* Ria. Retrieved March 1, 2022, from: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html

Republic of Estonia Ministry of Economic Affairs and Communications. (2018). *State information system*. MKM. Retrieved March 2, 2022, from: https://www.mkm.ee/en/objectives-activities/information-society/state-information-system

Republic of Estonia Ministry of Economic Affairs and Communications. (2021). Digital Society Development Plan 2030. MKM. Retrieved March 22, 2022, from: https://mkm.ee/et/eesmargid-tegevused/infouhiskond/digiuhiskonna-arengukava-2030

Republic of Estonia Ministry of Economic Affairs and Communications. (2020). *Cyber Security*. MKM. Retrieved March 3, 2022, from: https://www.mkm.ee/en/objectives-activities/cyber-security

Republic of Estonia Police and Border Guard Board. (2018). *Estonian eID scheme: ID card.* European Commission. Retrieved March 1, 2022, from: https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20ID%20card.pdf

Riigikogu. (2017). *Emergency Act*. Riigi Teataja. Retrieved March 9, 2022, from: https://www.riigiteataja.ee/en/eli/516052020003/consolide

Riigikogu. (2020). *Identity Documents Act.* Riigi Teataja. Retrieved March 1, 2022, from: https://www.riigiteataja.ee/en/eli/ee/526042018001/consolide/current

Runeson, P., Host, M., Rainer, A., & Regnell, B. (2012). *Case study research in software engineering: Guidelines and examples*. John Wiley & Sons.

The Security Identity Alliance. (2021). *Giving Voice to Digital Identities Worldwide - Key insights and experiences to overcome shared challenges*. Digital ID Working Group of the Secure Identity Alliance. Retrieved March 1, 2022, from:

https://secureidentityalliance.org/utilities/news-en/entry/giving-voice-to-digital-identities-worldwide-1-1

Valtna-Dvořák, A., Lips, S., Tsap, V., Ottis, R., Priisalu, J., & Draheim, D. (2021). Vulnerability of State-Provided Electronic Identification: The Case of ROCA in Estonia. *In Electronic Government and the Information Systems Perspective*, 12926, (Lecture Notes in Computer Science), 73-85.

Veldre, A. (2017). *ID card ecosystem*. Blog of the State Information System Board. Retrieved March 22, 2022, from: https://blog.ria.ee/id-kaardi-okosusteem/#comment-11091

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). sage.

Appendix 1 – Interview questions

Language: English

Time: approximately one hour

Interviewees: Public/Private sector experts

All interviewees were informed about recording.

Introduction:

Q.1. What are your current position and main responsibilities in authority?

Q.2. What is your connection with the eID ecosystem field? (Including years of experience)

Part 1 (Historical background):

Q.3. How did eID become a part of the Estonian state CI?

- Q.3.1. Why did eID become a part of the Estonian state CI?
- Q.3.2. When did Estonia understand that eID should become a part of the CI?

Q.4. In your opinion, what were the conditions that forced to add eID as a part of the CI?

Q.5. Which prerequisites showed the readiness of eID to become a part of the CI? (Name up to 3)

Q.6. Please name some of the critical changes (including risk management) that followed since eID became a part of the CI?

Q.7. What was the most challenging part in the process of making eID a part of the CI?

Q.8. How do you think, did eID become a part of the CI on time or too early or too late? Why?

Part 2 (eID As-Is):

Q.9. Which eID ecosystem components/elements are critical according to the following common critical criteria:

- Q. 9.1. Proportion (number of elements)
- Q. 9.2. Time (react, restore the functionality)
- Q. 9.3. Quality (the quality of service delivery)

Please, assess each of your component/element criticality on a 10-point scale, where 1 means that the element is not critical and 10 means that the element is highly critical in the eID ecosystem.

Q.10. What are the technical resilience components which may reduce the vulnerability of eID towards disruptive events?

Q.11. What are the organisational resilience components which may reduce the vulnerability of eID towards disruptive events?

Q.12. In case of the eID failure, how the critical risks are managed in the ecosystem and what are the main elements in the risk management process?

Q.13. What is the role of PPP in eID CI management in Estonia?

Part 3 (Further development):

Q.14. Do you think the eID ecosystem should be a part of the state CI?

Q.15. In your opinion, what are the key elements to identify that eID should be a part of the CI?

Q.16. What are the main advantages and disadvantages of eID being a part of the CI?

Q.17. In terms of eID, what preconditions must the country fulfil before making eID a part of the CI?

Q.18. What do you think are the most important takeaways from the Estonian case?

Q.19. Is there anything that you would like to add?

Appendix 2 - Explanatory final checklist

Define whether eID is critical for society by looking at critical requirements` indicators:

Indicator	**Elements**	**Description**
Dependency	Society, IT systems, e-services, vital services.	eID became a part of citizens' daily transactions in the public and private sectors.
Necessity	Crisis impact	The risk of crisis results from system vulnerability or security issues.
Cooperation	Banks	Banks are interested in secure authentication methods for online banking.
Law	EU regulation, national regulation	The electronic signature is equal to the paper signature, and authentication options are integrated into the government system, which requires legal high-security assurance.
	Personal data	A large amount of personal data belongs to the government.
Other	e-Residency	Significant enabler, which gives a critical value.

Necessary preconditions to complete from the government side:

Preconditions	Elements	Description
To set up the eID approach	Physical document (card), IT solutions (user software).	To connect a person with an electronic environment by applying a physical person identity to an electronic identity.
Law	Identity document	Citizens must hold an issued by a state authority national identity document.
Security	Cyber security	Cyber security strategy for CI and vital services is a part of security information systems to sustain a digital society relying on cryptographic solutions and transparency.
Trust service	Digital certificates	Qualified service providers which legally comply with trust service provision requirements.

eID critical resilience elements, the failure of which make a significant impact:

	Elements	Description
Technical	eID tokens	To develop and integrate electronic alternatives to ID cards.
	Standards and policies	To update the legal framework, which ensures legal certainty for the ecosystem

		participants supported by a technical lawyer advisor.
	Trust Service	Regulated and provided by the national qualified service provider.
Organizational	Risk Management	To embed external and internal regularly audited risk management based on the law requirements.
	Public-Private Partnerships	Mutual engagement of stakeholders and partners from the private sector for long-term sustainable development to strengthen risk management and share common values are part of national security to facilitate CIP.
	People	To support and regulate different organizational structures and coordination between and inside the organization based on policies.

Appendix 3 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Karolina Bejussova

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Assessment of the eID Ecosystem as a Part of the State`s Critical Infrastructure: the Case of Estonia”, supervised by Silvia Lips
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

09.05.2022

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