TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Astrid Valtna-Dvořák
178204IVMG

ROCA VULNERABILITY AND STATE-PROVIDED ELECTRONIC IDENTIFICATION: CASE OF ESTONIA

Master's thesis

Supervisor:	Dirk Draheim
	Prof. Dr.
Co-Supervisor:	Valentyna Tsap
	MSc.

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Astrid Valtna-Dvořák
178204IVMG

ROCA TURVANÕRKUS JA RIIGI POOLT PAKUTAV ELEKTROONILINE ISIKUTUVASTUS: EESTI JUHTUM

Magistritöö

Juhendaja:	Dirk Draheim
	Prof. Dr.
Kaas-juhendaja:	Valentyna Tsap
	MSc.

Tallinn 2020

Author’s declaration of originality

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

Author: Astrid Valtna-Dvořák

27.07.2020

Abstract

The purpose of this thesis is to provide a detailed overview of the 2017 ROCA case in Estonia and to understand what implications does this large-scale security risk pose on on a fully rolled-out State-provided eID scheme. The analysis focuses on three areas: the State's political tasks and responsibilties; the role if the ICT industry in the eID provision process; and thirdly, the opportunities and obligations for the end-users, including the State itself as the primary end-user of the eID.

This thesis contributes a thematic analysis of 32 semi-structured interviews conducted with 41 Estonian high-level experts closely involved in solving of the 2017 ROCA case in Estonia. These interviews provide a deep insight into the crisis management process as well as into the characteristics of Estonian eID area.

The author's proposals for further discussion on eID management includes rethinking the definition of eID in the light of the Estonian example and acknowledging the paradigm shift that already has taken place in Estonia for recognising the electronic identity as the citizens‘ right and its provision the State's obligation.

Keywords: Return of the Coppersmith's Attack vulnerability, ROCA, eID management, state-provided eID, e-ecosystem, eIDAS, State, qualified Trust Services, large-scale security risk

This thesis is written in English and is 94 pages long, including 8 chapters and 4 figures.

ROCA turvanõrkus ja riigi poolt pakutav elektrooniline isikutuvastus: Eesti juhtum

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 94 leheküljel, 8 peatükki ja 4 joonist.

Acknowledgements

I am glad to acknowledge the TalTech Centre for Digital Forensics and Cyber Security research group led by Prof. Dr. Rain Ottis for designing and creating the initial body of research about the 2017 ROCA case in Estonia. I am grateful for your trust and making the interviews available for my thesis. This thesis is directly based on the interviews that were designed and conducted by Rain Ottis' research group for the purpose of their research project.

I wish to deeply thank Martha Jung, a vital member of the research group and a co-author of the TalTech report *"ID-kaardi kaasuse õppetunnid"* for her input, especially for producing the transcriptions and Estonian-English translations of the interviews.

I wish to thank Prof. Dr. Dirk Draheim for his trust, patience, and guidance. Especially great thanks to MSc. Valentyna Tsap for her steady support and valuable insights, as well as to TalTech's e-Governance team for their hands-on and optimistic mindset throughout this process.

I want to thank my family for their everlasting support. Without their willingness to help and adventure, this journey would not even have begun. I wish to express special thanks to Kateřina for offering me a safe haven to work in.

List of abbreviations and terms

CERT	CERT-EE (Computer Emergency Response Team Estonia)
ECC	Elliptic curve cryptography
eID	Electronic identity, digital identity
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ETO	Vital Service provider (Elutähtsa teenuse osutaja)
EUTS	Electronic Identification and Trust Services for Electronic Transactions Act (E-identimise ja e-tehingute usaldusteenuste seadus)
HOS	Emergency Act (Hädaolukorra seadus)
HOLP	Emergency Resolution Plan (Hädaolukorra lahendamise plaan)
mID	Mobile-ID
MKM	Ministry of Economic Affairs and Communications
MS	European Union Member State
PPA	Police and Border Guard Board
RIA	Information System Authority
SiM	Ministry of the Interior
SK	SK Identity Solutions AS
SMIT	Information Technology and Development Centre of the Ministry of the Interior
STAK	Internal Security Development Plan (Siseturvalisuse arengukava)
TalTech	Tallinn University of Technology

Table of contents

List of figures

1 Introduction

The 2017 ROCA case presents significant implications for the Estonian national security and electronic identity management. It is a unique case in the Estonian State administration that put on test its ability to rapidly react to a large-scale security threat; provided valuable lessons to learn and indicated several areas that need to be developed further in order to minimise such risks for the Estonian State in the future.

1.1 The 2017 ROCA case in Estonia – an overview

On August 30, 2017, Estonia was notified about the ROCA (Return of the Coppersmith's Attack) cryptographic vulnerability on the chips used in the Estonian ID-cards. According to the research group that discovered vulnerability, the RSA (Rivest-Shamir-Adleman) cryptographic keypair generation in chips consisted a fault. This allowed their private key to be derived from the public key, potentially allowing for a malicious misuse of any of the affected ID-cards (Information System Authority, 2018b). The ROCA vulnerability affected an estimated minimum of 1 billion chips around the world in a variety of computing devices and on plastic cards (driving licences, passports, access cards etc.). Despite that Estonia's affected 750,000 ID-cards make up a negligible share of the 2017 ROCA case's global impact (Nemec *et al.*), the Estonian case was exceptional due to the significance of the ID-card for the Estonian State administration and business environment.

It was quickly understood that the ROCA vulnerability represented a threat to Estonian national security. The Estonian ID-card is a physical identity document which also carries the individual's digital identity – the eID. Approximately two thirds of the Estonian ID-cards, those issued after October 2014, needed immediate exchange of security certificates (Information System Authority, 2018b). Due to the large number of the digital certificates affected and their broad use in both state and private sector services, revoking the cards would have meant extensive impact to the availability of or access to public services – such step would have disrupted the use of e-health systems, the digital services of Tax and Customs Board and the Government document exchange platform as well as financial transactions in the country. Work at and between government agencies would also have been disrupted (Ibid.). The impact on the private sector is harder to assess in precision, but the electronic identity connects the Estonian residents and e-Residents to over 3000 services (Information System Authority, 2019). This list is merely illustrative and not a complete overview of the impact the Estonian ID-card and the electronic identity has on the Estonian society, the State administration and the country's digital ecosystem as a whole. The materialisation of that risk would likely have had significant impact on Estonian economy and on the credibility of the State's administration.

The Estonian State faced such a large-scale security risk handling process for the first time (Lips *et al.*, 2018). The solution to the situation had to restore the security of the ID-card without affecting the availability of services. In essence, Estonian was set in a race against time in early September, looking neutralise the security risk before the scientific information regarding the ROCA vulnerability would be published on October 30, 2017 (Information System Authority, 2018b).

A solution based on the elliptic curve cryptography (ECC) was chosen to replace the RSA library and implemented on the ID-cards. The solution was implemented by a software update which then enabled the certificate renewal procedure either remotely by the end-users or in the PPA service points. Owing to the widely dispersed pre-existing software and hardware solutions (ID-card software and ID-card readers) among the eID user base, the remote renewal option was widely used and allowed Estonia to avoid having to exchange a large number of affected ID-cards (Lips *et al.*, 2018; Information System Authority, 2018b).

The risk handling process, referred to hereinafter as the 2017 ROCA case in Estonia, revealed many aspects about the provision process and supply chain of the Estonian ID-card. Moreover, the vulnerability showed how dependent the Estonian society is on the ID card. The case demonstrated the crisis management capacity, methods, and organisational complexities of the Estonian State administration. It also revealed the prevalent user behaviour and user attitudes towards the digital identification in Estonia.

Although the ROCA case pinpointed a variety of factors influencing the provision of the eID service, the case was essentially recognised as security issue. Indeed, it is unimaginable to discuss electronic identification without a strong emphasis on its security mechanisms. Security is a characteristic that is deeply ingrained in the electronic identification process. Consequently, security is not presented as a part of a research question in this thesis but is analysed as one inseparable aspect of the Estonian eID phenomenon.

1.2 Research problem and purpose

The question of electronic identification is becoming more and more relevant globally. Many societies, business entities and governments are building up or redesigning their operational processes upon the functionalities of digital identification, authentication, and the use of digital signatures.

This leads to the more specific research problem at hand: the usage of electronic identity unavoidably causes wider socio-technical effect (van Dijck and Jacobs, 2020; (Hedström *et al.*, 2015); Latour, 1990).

Initially, the term socio-technical accentuated a close association between the technical and social systems within organizations and was coined due to the need to redesign jobs in the industrial setting to make work more fulfilling for the industrial era workforce. The new approach in socio-technical research shifts the focus on social settings; and therefore forms a bridge between information systems research and social sciences. That is to say, socio-technical principles strive to truly accommodate the interplay between the technical and the social sides of information systems (Ghaffarian, 2011).

Moreover, the widespread use of state-provided electronic identity is innately related to modern models of e-government; the interplay and setup of institutions within and beyond a nation state, including the market actors with their unique set of interests and contributions. Hence, a multi-levelled and complex scene emerges when the provision of national electronic identity is explored.

A model for institutional design for complex technological systems that is proposed by Koppenjan and Groenewegen (2005), is considered vastly relevant for describing e-government systems and e-government ecosystems, among other systems (Bharosa *et al.*, 2020). Firstly, this model incorporates three different design processes. The technological design involving *"demarcation, components, relations, processes"*; the institutional design involving *"arrangements between actors that regulate their relations: tasks, responsibilities, allocation of costs, benefits and risks"* and the process design involves *"who participates in the design process; what are the conditions, rules, roles, items, steps, etc."* According to Koppenjan and Groenewegen, the way the design process itself is designed, plays equally crucial role as compared with the technological and institutional design. Given the complexity and varying number of actors, and with the interdependencies between them in an e-government (ecosystem), the importance of the process design becomes evident (Koppenjan and Groenewegen, 2005).

The model further distinguishes four layers of analysis to better grasp the functioning of complex technological systems. Each layer describes different kind of institutions *"with regard to the kind of things they address, the way they work and evolve, and the extent to which they can be influenced",* thus allowing to grasp the larger context in which the institutional arrangements form (Ibid.).

Estonia presents a prime example of e-government and thus the Koppenjan and Groenewegen institutional design model serves as a potential framework for gaining a deeper understanding of the functioning of the Estonian e-ecosystem and e-government model which heavily rely on the state-provided electronic identification. Looking at institutional design therefore helps to better understand also the eID provision and management processes.

Hence, the analysis of the 2017 ROCA case in Estonia is a well-fitting contribution to this scholarly discussion. Moreover, it provides a rare chance to explore what are the implications of a large-scale security risk on a fully rolled-out State-provided eID scheme.

The 2017 ROCA case in Estonia allows to explore how does a security threat in this area influence the State as the provider and the primary end-user of the electronic identification service? How does the State as an actor relate to other eID end users and as a sovereign actor on the international market for ICT services and products? What are the unique circumstances and characteristics of the Estonian eID?

The purpose of this thesis is to analyse the implications of the 2017 Estonian ROCA case on State-provided electronic identification. The analysis focuses on three areas: the State's political tasks and responsibilties; the role if the ICT industry in the eID provision process; and thirdly, the opportunities and obligations for the end-users, including the State itself as the primary end-user of the eID.

1.3 Overview of the thesis

The introductory chapter of this thesis gives an overview of the 2017 ROCA case in Estonia and the wider research problem deriving from that.

Specific research questions are outlined, and the research design and methodology are described in the second chapter of this thesis.

The related background information is provided in the third chapter in order to give the reader a fuller overview of the Estonian digital ecosystem and the current arrangement of the eID area, including the technological solutions in use along with the list of stakeholders.

The body of research, namely the substantial thematic analysis, and its conclusions are presented in the three following chapters. Chapter 4 presents the thematic analysis theme “State and policies” and its conclusions; Chapter 5 theme “Market and the EU” and Chapter 6: theme “End user,” respectively.

The “Conclusions and discussion” section concludes the research results and provides an answer to the main research question. An analysis of the scientific literature relevant to the research results is included in this section in order to offer context to and underline the relevance of the given work within the academic literature. The limitations of this research and a wide spectrum of topics for further research are presented in this section.

2 Research design and method

An in-depth study about the lessons learned from the 2017 ROCA case was commissioned by the Estonian State Information Systems Authority and carried out by the Tallinn University of Technology research group in February-April 2018. The study was concluded in the form of 32 semi-structured interviews with 41 individuals. The circle of interviewees included all experts that were the closest involved with the resolution of the ROCA case in Estonia and represented majority of the public and private sector stakeholders in the Estonian eID area (Information System Authority, Estonian Police and Border Guard Board, Ministry of Economic Affairs and Communications, Ministry of the Interior, Ministry of Foreign Affairs, Government Office, SK Identity Solutions, Information Technology and Development Centre of the Ministry of the Interior, Cybernetica AS and independent communication specialists). The main purpose of the study was to identify the lessons learned from the ROCA case and formulate a list of policy recommendations for practical implication. The main emphasis if this research was on eID management and crisis management aspects of the 2017 ROCA case (Buldas *et al.*, 2018).

This thesis analyses the above described interviews in depth, concentrating on the wider socio-technical implications of the ROCA case on State-provided means of digital identification. The main research question of this thesis is the following:

What implications does the 2017 ROCA case in Estonia present on electronic identification mechanism provided by the State?

The main research question was elaborated into three sub-research questions as follows:

1) Which political responsibilities for the State emerge from the case?
2) Which roles for the information technology industry emerge from the case?
3) Which obligations and opportunities for the eID end-users emerge from the case?

The primary research method is thematic analysis of these 32 semi-structured interviews. Thematic analysis is a foundational qualitative research method, designed to analyse rich textual data sets. It is a method for identifying, analysing, organizing, describing, and reporting themes found within a data set. *"A theme captures something important about the data in relation to the research question"* (Braun and Clarke, 2006).

The whole data set consisting of 32 semi-structured interviews was used and fully analysed in this research. Inductive, data-driven, approach was chosen for conducting the thematic analysis. Inductive analysis is a process of coding the data without trying to fit it into a pre-existing coding frame (Ibid.). The specific research question has evolved only through familiarisation with the interview data and saw modifications of certain nuances throughout the analysis process. The thematic analysis concentrates on 3 themes ("State and Policies", "Market and the EU"; and "End User") corresponding to the three sub-research questions posed by the author.

The themes and codes were formed semantically, resulting from their surface level meaning. The realist interpretation of those themes and codes followed in a later phase of the analysis process.

The first phase of the analysis of the interviews was done independently of scientific literature on electronic identification or any other related field. An overview of scientific literature was added to the final conclusions of the research results to better contextualise the author's findings in the relevant academic literature.

The thematic analysis was conducted in NVIVO qualitative data analysis software. According to Welsh (2002), computer assisted qualitative data analysis software allows the researcher to acquire accurate and transparent picture of the data whilst also providing an audit of the data analysis process as a whole.

Following is the description of the 6 phases of the thematic analysis according to Braun and Clarke.

Phase 1: Familiarisation with the data. In this phase, an overview of the whole content of the dataset was acquired.

Phase 2: Generating initial codes. The initial round of coding of all 32 interviews was carried out.

Phase 3: Searching for themes. Three initial themes were formed. These were named: “State & Policies”, “Technology & Partners” and “End User & Ecosystem”. The hierarchy of the code tree reached four levels and consisted of 70 separate codes (Appendix 1) and 1344 individual coding references.

Phase 4: Reviewing themes. This phase saw an adjustment of the code tree. The aim of the changes was to add precision into the themes respective to each sub-research question. Topics not directly related to the sub-research questions were placed in two additional themes. Codes related to crisis management were inserted into the “Crisis Management” theme and the codes describing the technological solutions that lead to the solving of the ROCA case in Estonia were inserted into the “Technology” theme. Some codes with similar meaning were merged and the code tree was rearranged to form only three layers of hierarchy. As a result, 1049 coding references and 63 codes remained to represent of the full coded data set.

Phase 5: Defining and naming themes. This phase saw a final refinement of the themes. As the topics of crisis management and policy recommendations were richly covered by the earlier research by A. Buldas et al., the respective theme was excluded from further analysis in this thesis. The codes in the “Technology” theme offered very shallow and fragmented overview of the topic and this theme was also excluded from further analysis in this thesis. Final names of the remaining themes were developed. The three themes analysed in this thesis are the following: “State & Policies”, “Market and the EU” and “End User”.

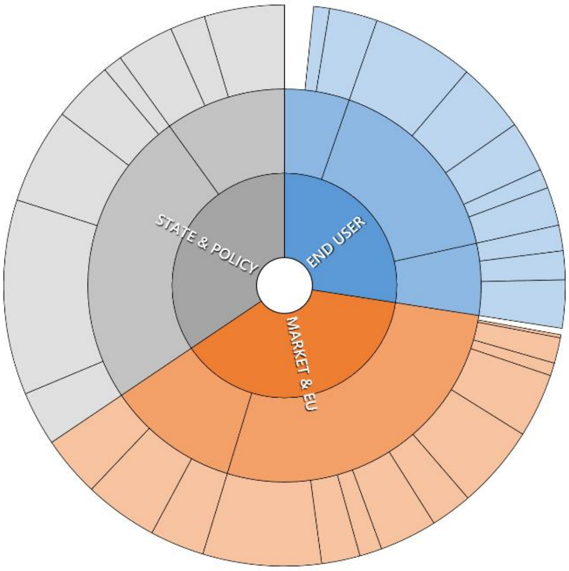


Figure 1. Proportional representation of the three final themes in coding references.

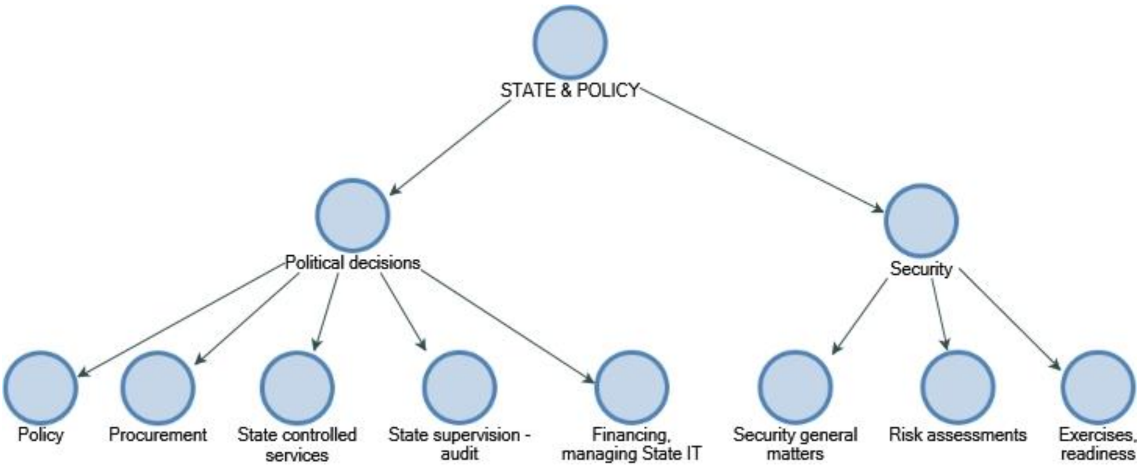


Figure 2. Theme 1: STATE & POLICIES.

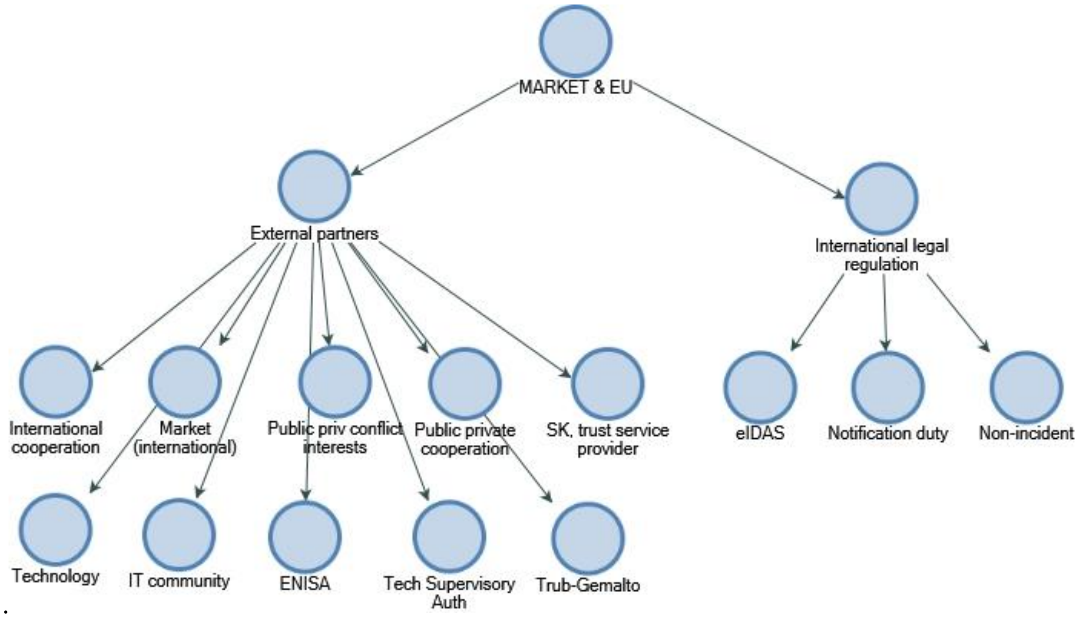


Figure 3. Theme 2: MARKET & EU.

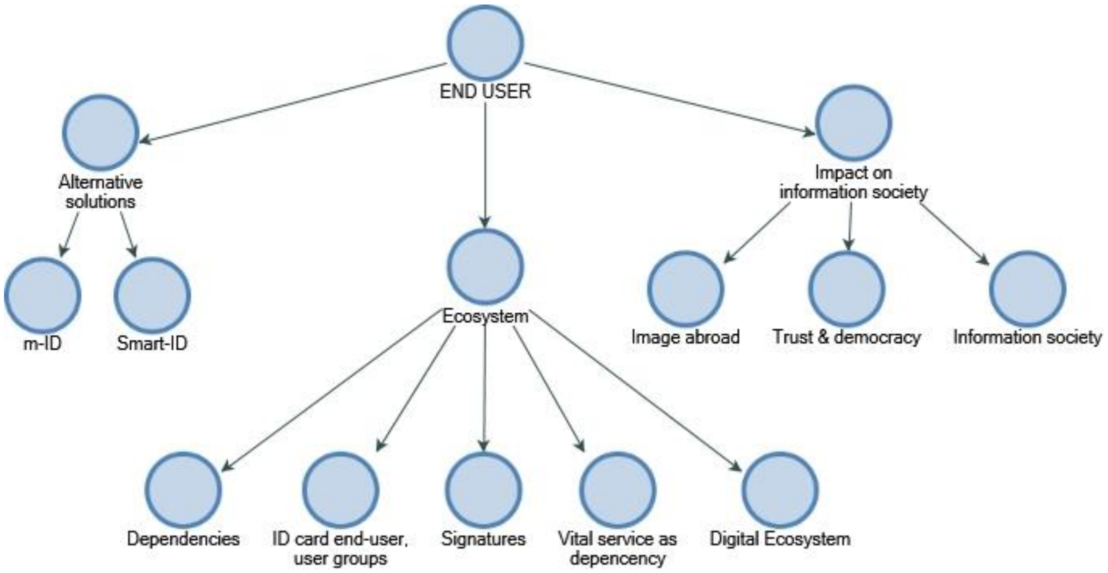


Figure 4. Theme 3: END USER.

Phase 6: Producing the report. In-depth analysis of the coded references was followed by compiling the highlights and core aspects into research report. The main research question and the sub-research questions were answered as conclusions of each respective theme.

3 Background

The importance of the 2017 ROCA case in Estonia is only understood if placed in the context of the Estonian digital ecosystem. Likewise, the large-scale security threat that the ROCA vulnerability posed to the Estonian national security and accountability as a digital government is only understood when knowing the focal place the Estonian ID-card and the digital identity document beholds in the Estonian information society and digital ecosystem.

3.1 Estonian e-ecosystem

Estonia has been praised by many authors for being an example of a successful e-State and a frontrunner in e-governance initiatives. Many countries and scholars are working to develop the e-governance concept even further. One of the latest additions to this discussion is the concept of Government as a Platform (GaaP). GaaP is suggested as a digital foundation for government to share data, software and services, and has been proposed as an efficient, effective and innovative model for government (Margetts and Naumann, 2016).

The Estonian digital ecosystem is being rated as coming close to the concept of Government as a Platform. The three layers that have been developed since 1999, give evidence of this concept. The three layers consist: a system of registries and data exchange that allow departments and agencies to share data (X-Road); a system of digital and mobile identification (eID) used by over 90 per cent of the population; and a service layer accessed through various front-end portals such as the official State portal eesti.ee (Ibid.).

The X-Road was developed as a secure internet-based data exchange layer that enables different information systems to communicate and exchange data with each other. The X-Road is secured by scalable KSI blockchain technology, developed to ensure The integrity and privacy of data stored in Government repositories (Enterprise Estonia, 2019). Despite that, some authors criticise it for having already become a legacy system for the Estonian e-ecosystem (Kattel and Mergel, 2019).

The Estonian ID-card is a physical identity document and a valid travel document. In addition, the ID-card is one of the many possible carriers of the Estonian eID.[1] The eID is a collection of data that connects the person with his/her physical identity in an electronic environment. In Estonia, each person has one physical identity and the same applies to electronic identity (Information System Authority, 2019).

The Estonian electronic identity operates on the basis of a public key infrastructure (PKI) which is based on a key pair – a secret key and a public key (Information System Authority, 2019). Since November 2017, the Estonian ID-card microchip is using 384-bit ECC public key encryption (Enterprise Estonia, 2020b) instead of the previously used RSA encryption library.

The impact of these fundamental e-governance infrastructure elements is explicitly visible in Estonia: More than 98 per cent of Estonian residents have an ID-card while approximately two thirds of the card owners use it digitally regularly. More than 3,000 public and private services use X-Road; the digital signature has been used almost 700 million times – as compared to the Estonian population of 1.3 million people. Among the most heavily used e-services are income tax filing and e-healthcare, not to mention financial transactions out of which nearly 100 per cent are made digitally. Likewise, nearly all personal income tax declarations are done online (98 per cent) and vast majority of health records (95 per cent) and medical prescriptions (99 per cent) are handled digitally. Last, but not least, the Government Office works paperless and on average 30 per cent of votes in both local and national elections are cast digitally (Enterprise Estonia, 2020a).

The Estonian government claims that its e-government infrastructure has annually led to savings of about 2 per cent of GDP and more than 800 years in working time for public and private sector in a calendar year (Kattel and Mergel, 2019). This indicates that *„some resources are beneficially redirected“* (Drechsler, 2018) within the Estonian economy owing to the broad use of the e-services, e.g. the State has invested in the

[1] Other eID carriers are residence cards, diplomatic IDs, mobile-ID, Digi-ID, and an e-resident’s Digi-ID.

digital infrastructure and to areas related to it, which generate higher value for the society than investing the same resources in public service provision in its traditional sense.

3.2 eID management and supply chain

The general framework of identity management in Estonia is formed by international and domestic standars and regulations, market competition, identity management organisational setup within the State, as well as policies and infrastructure related to the eID service (E-Estonia Council, 2018).

The Estonian eID ecosystem is composed of the following institutions and public and private sector stakeholders:

- The Police and Border Guard Board (PPA) is responsible for authentication and identity management; procures identity documents and guarantees their issuance.
- Estonian Information System Authority is responsible for the development and management of the electronic identity software and Trust Service infrastructure. In addition, the RIA is responsible for cyber security in the eID area.
- The SMIT is developing, procuring and managing the information and communication services of the Ministry of the Interior; this includes ICT services connected to identity management and identity documents.
- Ministry of Economic Affairs and Communications initiates and coordiantes Estonian information society policies.
- Ministry of the Interior works out the policy for identity management and identity document issuance (both for Estonian citizens and residents).
- Ministry of Foreign Affairs guarantees that the interests of Estonia and its citizens are protected abroad; as well as accepts applications for and gives out indetity documents.

- Consumer Protection and Technical Regulatory Authority carries out supervison in the field of information society services and Trust Services.

- Enterprise Estonia is responsible for the e-Residency programme and creates favourable conditions for developing services and organises information exchange with Estonian e-residents.

- Private sector qualified Trust Service provider that cooperates with the Estonain State in trust service provision.

- Telecom operators that issue Mobile-ID enabled SIM cards to their clients.

- Private sector based identity documents provider that cooperates with the State in producing identity documents and in personification of these identity documents (E-Estonia Council, 2018).

These above listed actors in their mentioned roles make up the Estonian eID supply chain and eID area managing institutions.

4 State and Policies

This chapter analyses the first theme of the thematic analysis: "State and Policies" and is divided into two sub-topics: Policies and Security. Each sub-topic summarises a number of codes that originate from the thematic analysis.

4.1 Policies

This sub-topic analyses the thematic analysis codes that depict national policies related to eID management, crisis management and financing the State ICT sector.

4.1.1 eID management

The Estonian e-ecosystem is based on two pillars: the interoperability framework x-Road and the eID which enables safe electronic authentication and giving certified digital signatures. It was underlined in the interviews that given the exceptionally broad-range and frequent electronic use of the Estonian ID-card, the concept of identity has changed from a travel document to a multi-use electronic authentication tool in Estonia. *"I agree that identity is not just "I am me" as a travel document is. It is more like an electric plug, where you can put your lamp, phone, hair dryer etc. The state has to offer this and guarantee it is secure."*

The eID is a fundamental part of the Estonian State administration. It is a basic infrastructure that enables the rest of the State functions to be executed in a smooth and economic fashion. The electronic identity has become the core value and primary enabler of the Estonian digital ecosystem.

The concept of a digital identity is unshakeably ingrained in the Estonian society and further developments of the eID are being discussed, which would elevate the provision of the e-services to a new level. The next steps involve the m-ID, the Smart-ID and the digi-ID: a cardless form of digital identity document. *“We had an idea, that if we have to exchange all e-residents’ cards, then we could jump to the new era: digi-ID, cardless.”*

It emerges that this fundamentally important area for the State is not under a consolidated development, management nor financing. The key concern for the State is the uncertainty about which of the State institutions is responsible for the eID and its development. *“We provide basic infrastructure as a State, the responsibility for it shouldn’t be so scattered. Every area can simply choose themselves how or what they do, plan their finances etc., both for eID and for x-Road. That’s not good.”*

Amendments to the Estonian legislation are being prepared in order to better define the roles in the eID supply chain. It is vital that the two leading ministries, the MKM and the SiM coordinate their responsibilities on the State level. Security related topics such as cyber investigation, reside within the SiM’s domain. The PPA, as the SiM’s subordinate organisation, is the issuer of the physical ID-card document. The person’s identity data is therefore also managed by the SiM and its subordinate bodies. The MKM is responsible for aspects of the eID which have an economic impact while the RIA, as the MKM’s subordinate body, takes care of the technical aspects of the eID and the ID-card production. *“We also have to think through what everyone’s roles and responsibilities are. Who is responsible for e-ID? I believe it should be more in MKM and RIA’s side, but we still have some things in SiM’s and PPAs side. Maybe we can assemble this system differently. Co-operation is much needed; vagueness is in no-one’s interest.”*

It is proposed in the interviews that each operational field of the State has to have a leading institution. That principle would also apply to the eID field. A leading institution is considered to be the owner of a given field and is also responsible for mitigating the risks in that field. It was suggested in the interviews that the RIA is *de facto* the service owner and thus should *become* the institution that has the leading role in the eID development and risk management. This would mean that the eID and ID-card related competences including the chip application and the oversight of the certification process need to be under RIA's domain. It was stated that concentrating these elements under one institution would help the State to set fitting requirements to the external service providers and ensure secure and optimised development of the ID-card. *“The implementing institution is the owner [of the eID service], not the ministry. So, the implementing institution has to own those risks.”*

The SMIT is a unit of the Interior Ministry which is designed compile the Interior Ministry’s IT competences into one single unit. The interviews revealed that there is a discrepancy between the expectations and the contribution to the State IT-development and maintenance of the SMIT. The development of the SMIT was not carried out fully because no political consensus regarding the SMIT’s areas of responsibility was reached. As a result, the SMIT has been left without political steering, appropriate funding and is undermanned for carrying out the statutes it was given. *“The SMIT should have more resources, to react faster, especially to small development, that are necessary very quickly.”*

The ID-card competence was initially envisaged under SMIT’s responsibility as the Interior Ministry is responsible for the ID-card production. In reality, this competence was handed to the RIA as the SMIT had not gathered the necessary capabilities for dealing with this area.

A discussion emerges from the interviews whether the IT capabilities of the PPA should be returned from the SMIT to the PPA or remain in the SMIT. Bringing the development back to PPA would allow the IT developments be tailor made for the PPA‘s needs. On the other hand, such solution is likely to separate the development from the maintenance and management tasks that are carried out by the SMIT. Some interviewees stress that the same organisation should coordinate the management and development tasks to guarantee durability and security of the IT-systems. *„Development and management in different institutions leads to not wanting to administer bad quality developments. Then conflicts might rise (who has to fix the bad quality developments?).”*

The discussion evolves further as the MKM has been considering the creation of a separate State IT institution. However, the interviewees fear that this would require too many qualified experts to start working at once (200 people). Alternative solution would be contracting experts from other ministries at the time of need; however, this would be an unsustainable solution for crisis conditions. It was concluded that an institution-centred management models do not serve the State’s current needs anymore. Instead, an inter-agency operative management model which would enable all the stakeholders to cooperate in crisis management is suggested by the interviewees.

Throughout the crisis solving process, the PPA and the RIA underlined that the electronic identity management policy is entirely missing in Estonia. So far, there is a single general document called the Internal Security Development Plan (STAK) drafted by the SiM. A strong divide in opinions whether the STAK serves as a sufficient political framework for comprehensive development of the eID area or not was expressed in the interviews. The PPA suggests that a more detailed plan, which would outline the direction for the eID area development form 5-10 years ahead, is needed. With this reason, the PPA, RIA and MKM launched the drafting of a more detailed strategic plan for the eID field, called: "Identity Management 10-year Vision". The initial working group includes other ministries (i.e. the MFA and SiM) and private sector partners.

It became evident from the interviews that differences in organisation culture and working methods hinder the cooperation between the four key institutions involved in the eID management (Interior Ministry and the PPA, RIA and MKM).

4.1.2 Crisis management

According to the Estonian Emergency Law, the cyber crises are to be solved according to Emergency Resolution Plan (HOLP). However, it was implied in the interviews that the ROCA case was approached and solved very much in an *ad-hoc* manner. A combination of reasons was mentioned by the interviewees. First, as not one incident of breaking the Estonian ID-card encryption occurred, the ROCA case was defined merely as a "threat" and a "risk which did not realise". Thus, none of the formal emergency resolution protocols were put into use. Announcing state of emergency was seen as undesirable, as a means of last resort. Instead, an informal crisis resolution plan was created on the go as the ROCA case was being solved. *"What are the documents followed in a cyber-crisis? 1) HOLP; 2) no-one wants to announce an emergency, so there's an informal "this*-is-not-a-*crisis" protocol."*

Secondly, the legal acts that regulate the eID area in Estonia are not harmonised and not fully adapted to the State's digital capacities. Furthermore, there is no single responsible State institution responsible for the eID area. Instead, there is a shared responsibility whereas respective inter-organisational crisis management protocols of the State are not worked out.

In a small organisation that has a wide spectrum of responsibilities and tasks - as the Estonian State may be described - handling novel or a crisis situation on an *ad-hoc* basis is often the natural course of events. On the other hand - as it is also the case with the Estonian State – certain emergency procedures are set up by the legal acts. Likewise, exercises are being held regularly in Estonian State administrative bodies to increase incident preparedness. During those exercises certain operational models are being learned. It was pointed out, that with those variables in place, approaching a crisis situation on an *ad-hoc* manner renders the above-mentioned efforts useless. *"Then we don't need HOS. We make plans, exercises and if something happens, then we deal with it completely differently."*

The *Ad-hoc* approach worked well for the Estonian administration because the people knew each other well and knew also their capabilities. The work ethics was very high. People took initiative and were willing to contribute far more work than regular working hours would have suggested (despite the state of emergency was not declared). Likewise, the private sector stakeholders offered their help and expertise. Clearly, in a bigger organisation or a State, such model for cooperation may not always be applicable and a more rigid approach has to be taken which would follow previously set up operational models and legal acts. *"I'd like to think that the reason why this crisis management was so painless for us, although mistakes were also made, was that we all knew people on all work lines, knew the capabilities etc." "Good work-relationships between people helped to solve the crisis."*

4.1.3 Managing public sector ICT investments

An evolvement of the Estonian digital ecosystem over the past 10-15 years emerges from the interviews. The early developments of the Estonian e-State were made gradually and often on *ad hoc* basis. It emerges from the interviews that Estonia has reached a phase of maturing. This is demonstrated by the organisational rearrangements that are being called for as well as by shifting the focus from constructing the ICT infrastructure one element at a time towards purchasing ready-made solutions and putting stronger emphasis on maintenance of the digital ecosystem. Calls for more thorough planning and an increase in investments are made by the interviewees. *"The e-State is hacked together somehow, and things are done in a: "ask that guy, he knows" style. We're in the point to start fixing it." "In the beginning we were building the car ourselves, now we need to keep the system working, but we buy the cars."*

A question of financing the State IT strongly emerged from the interviews. It is clearly expressed by the interviewees that the State has underestimated the importance of investing in the State's digital ecosystem for years. First and foremost, the State's dependency on the digital ecosystem must be acknowledged and backed up by financial means accordingly. It appears that the functioning of the State's digital framework has been taken for granted in great extent. It can therefore be inferred from the interviews that the more guarantees the State gives to its citizens about the e-services – about these services being secure and reliable – the more the State has to invest in order to make these promises true. ICT-expenses are rising all the time which makes the budgets increasingly difficult to balance. *"IT-society, IT-systems – it needs more finances than so far. We have made ourselves dependent of it and need to come to terms that it is going to take a lot of resources."*

Keeping up the e-State is expensive not only in terms of financial resources but also in qualified human resources. The interviewees stress that human resources dedicated to this highly important topic for the Estonian State, are scarce. Such comments were primarily made about RIA, PPA and SMIT. Capabilities are missing in cryptography area as well as analysts and experts familiar with the ID-card production and eID field in general. The circle of people holding the knowledge is very small. This poses a certain risk regarding how sustainable the State is in terms of competence and expertise. Moreover, there is a need for a stronger political consensus on how the ID-card related matters are being handled. *"If now the state would understand that this is an expensive area, the technology is expensive and developing, we need new people who know the new technology, who can ensure the security elements etc. If the State would understand it, it would be a huge step."*

People working in the eID field are overloaded with work and manage to work on the most urgent tasks only. The forward-looking lines of work are suffering because of that. It was also stated in the interviews that there is not enough people that could participate in policy making on the European level by working out suggestions to the European legislative bodies and ENISA. *"I'd say bigger capability do work with the ID-card or the document, technical or overall knowledge. We put a lot of resources into dealing with 'situations', problems, but we can't develop the field enough, this is where the problems arise."*

The State as an employer is in a challenging position because it has to compete with the private sector companies for limited amount of competent workforce. Based on the statements made in relation to RIA, it becomes clear that the investments into human resources should be complemented with appropriate remuneration, optimised workflow, and administrative burden as well as skilful management. There are certain positions in the State IT departments that are difficult to fulfil because some State institutions have an unfavourable reputation or certain positions require a skillset that is difficult to attain from the labour market.

It was suggested in the interviews that the State could also benefit from an ability to scale up its IT capabilities as the need arises. This may mean hiring extra people as needed or simply buy in the capacity at times when the workload increases rapidly but temporarily. Here, close ties with the Estonian IT community (experts from academia, private sector, former State sector employees and other competent organisations) could facilitate these efforts. Increasing funding for science and universities was also mentioned as an indirect means for combating the lack of competent workforce in the (State) IT sector.

Despite the lack of overall funding of the State IT area, finances were not in the way of solving the ROCA case. The interviewees stated that ample funds were made available as soon as the need arose. *"The government said that we can spend as much as is necessary and that took off some worries for sure." "No, nothing was left undone because of money."*

4.2 Security

This sub-topic analyses the codes related to security aspects of the eID provision.

Readiness for crisis depends on exercises, mapped critical services and infrastructure as well as realistic risk assessments that are being backed up by sufficient strategic preparedness, the know-how and resources. Another aspect of security provision is the involvement of the private sector entities in the development of the State ICT systems and services provision.

4.2.1 Security

The interviews revealed that the State does not have enough personnel capable of assessing security risks at a deeper level on the eID field. With regard to the ROCA case, there was only one person working for the State institutions who had the expertise necessary for understanding the risk posed by the ROCA vulnerability. *"The security officer also has to understand these things though. Officer X could have understood, if he wouldn't have had other things to do at the time. Probably he was the only one."*

It was inferred to in the interviews that security is being approached as a separate topic while developing the State ICT systems, not as a fundamental part of the systems and services. *"Many things are developed in such way, that security is just an afterthought."*

From security perspective, the interviews revealed an important shortcoming. Both alternative authentication tools available in Estonia during the ROCA case: the ID-card and the DigiDoc service, were relying on the same certification provider, SK. Thus, the State's dependence of SK was identified as a single point of failure. The need to diversify the range of service providers was noted as one of the key priorities for the State thereof. *"One of the lessons we learned from this crisis, we have two options for authentication: ID-card and DigiDocService (offered by SK), which also offers both methods: mID and Smart-ID. This is one point of failure, if something should happen to SK: political, legal attack, doesn't go through the security* audit, *loses the Trust Service level, owners sell the company...."*

It was also stated that there is a need to gather cyber security related competences and responsibilities under one organisation. For the time being, Cyber security related political coordination is in the realm of the Ministry for Economic Affairs and Communication. Yet, there is not enough knowledge and political leadership (and interest) for coordinating the activities which should result from this political steering. The RIA has been suggested as the institution that could take on this role, however, lack of personnel was quoted as the primary obstacle. *"So, it should have coordinative function, management function and the right to make political choices: this is the way we're going to implement security."*

Until the cyber security related competences remain scattered among different institutions, and with interoperable ICT systems in use, the only possibility for effective security provision lies in cooperation between all the institutions involved.

4.2.2 State controlled services

A discussion regarding which services on the ID-card supply chain should be under State's control emerged from the interviews. Contrary to the national passport, which the State produces itself, the Estonian State is fully dependent on private service provider when it comes to the production of the ID-card. Potential security risks are associated with this dependency. *"We could do the same with the ID-card: buy the equipment, the blanks and separately the certification."*

The State has specific needs which do not necessarily match with the commercial products offered on the market. The State needs to have control over certain part of the ID-card production process to ensure the confidentiality of the identity document data. The service providers may not be interested in modifying their products or production processes to match the interests of a small client like Estonia. *"You can get the cards from wherever; the blanks can be provided by anyone. The question is, where you personify it. Where do you get the digital part and certificates (Trust Service side)."*

With respect to the ID-card production and the respective software application, opinions vary. The key arguments in this discussion include reliability of the service provider and economic effectiveness. The State would like to have these service under its control, yet, it is economically more efficient to procure a ready-made solution from private producers. The requirements regarding confidentiality and security are guaranteed by solid contractual base and domestic legislation.

The State is the most worried about its dependency on the certification provider. It would be easier for the State if the certification was under State's control. However, it would require the respective expertise and would thus pose another responsibility. The Estonian State is strongly dependent on the SK as the certification provider. Some interviewees express a strong concern that such a company should only be Estonia-based. The certification service if a crucial element of the ID-card production which, in the hands of a private company, Estonian State has no influence over. *"Either it should be state-controlled officially or not, but it should be on Estonian territory and be closely connected with the state."*

4.2.3 Exercises

Exercises play a fundamental role in crisis preparedness. The lessons learned from the exercises help to prepare operational plans and to place the necessary resources in the disposal of the responsible institutions. *"We have to have exercises, write and play through these situations, to know who makes operative decisions, where the stationary headquarters is etc."*

Several exercises have been organised concerning the failure of an element of the State ICT solutions. An earlier exercise with a very similar scenario as the ROCA case took place in 2015. Back then, the scenario was considered unlikely by the participants and the exercise was not taken seriously. No action plans resulted from that exercise, only vague political guidelines to "find out responsibilities" were put in the Government's work plan. *"In 2015 there was a bigger exercise where we played through a situation where 390 000 certifications were faulty."*

One of the reasons why the 2015 exercise failed was said that it remained on a theoretical level. Then, 390 000 certificates were revoked easily but the real effect of such an act did not become clear to the participants. Practical and operative exercises are needed to bring the real feeling of a crisis to the participants. However, finding an appropriate landscape for holding a practical exercise may prove difficult as playing those scenarios through on the real digital ecosystem is not considered possible. *"Training is necessary, but where to do it? We need an exercise field, to play on the real ecosystem is …. Risky."*

The interviewees have suggested learning from the ROCA case, as well as making more exercises to increase the preparedness for future crises. The future exercises should also be focused at crisis management itself and be organised across multiple organisations to allow for better inter-organisational cooperation. Exercises must be held at a sufficient frequency to respond personnel changes in the State institutions. There is little use of exercises if the people who participated no longer work for that particular institution. The more critical areas for the State should be prioritised also in the scenarios for the exercises. *"This crisis can be used as an experience and make conclusions. We should play through the same situation in exercises; it won't be our last crisis."*

Some respondents have said that the crisis handling could not have been better, with or without any exercises held. The solution for overcoming the ROCA case was worked out rapidly. *"On Thursday we had the first meeting in RIA, on Friday the first technicians' group meeting, then ministries. Saturday-Sunday we worked; on Monday morning we knew the solution. When the Prime Minister said the solution will come in 2 months, it was not random. I'm not sure if an exercise would have helped to do this better."*

4.2.4 Risk assessments

The risk assessments that existed prior to the ROCA case proved to be insufficient and unrealistic, by excluding very plausible scenarios. It was pointed out by the interviewees that people only start believing that something can go wrong in the State ICT sector when something really does break up. Such behaviour is not far from negligence from the perspective of safeguarding and guaranteeing continuity of the State e-services. *"All the time there has been talk that one of the risks is that crypto will weaken or be broken. It was unbelievable. Maybe not discussed enough."*

Moreover, mapping all the ID-card dependencies has a strong security implication. It is difficult to guarantee the security of the State-provided e-services when a comprehensive picture of those services is missing. This includes the services that are dependent on the ID-card.

Given this, the State had no overview how big threat it was facing at the onset of the crisis. The risk assessments related to the ROCA case were compiled as the situation evolved, involving the contribution of public and private sector stakeholders. *"Assessment of the impact on the economy, on the e-State – this is MKM's work. Security risks, effects on criminal behaviour – this is PPA's, SiM's and Estonian Internal Security Service's."* Further information was acquired from RIA, Cybernetica and CERT.

4.3 Conclusions of the theme "State and Policies"

This section provides an answer to the sub-research question: Which political responsibilities for the State emerge from the case?

The theme "State and Policies" reveals that the concept of identity has changed in Estonia from a travel document to a multi-use electronic authentication tool. The concept of a digital identity is steadfastly ingrained in the Estonian society. Further developments of the eID are being discussed, reaching even to a cardless form of a digital identity document.

The Estonian State has taken a steadfast direction towards more reliance on the eID and more projects in the digital realm. The Prime Minister's supportive political message at the early stages of the ROCA case, the Government-led future looking eID developments, and the funds made available to resolve the ROCA case, demonstrate the importance of the eID for the Estonian State. With this political support and the broad extent in which the eID has been taken into use in Estonia, there is a justified expectation from the residents for the continuation of the eID service.

The State's guarantee for the safety and durability of the eID in Estonia is unprecedented. Indeed, it is the cornerstone of the Estonian State administration. Along with the x-Road, the eID is the primary enabling element of the country’s digital ecosystem. It appears that not only Estonian residents are the end users of the eID but also the Estonian State itself. There are public services which the State is not anymore able to offer in a non-digital version and thus, without the use of the eID.

The Estonian State has made itself so dependent on the eID, that the State, the whole digital ecosystem and in some cases, human lives, depend on the continuous and flawless functioning of the Estonian eID. The eID serves as an underlying enabler of a wide range of public services, the Vital Services, and the country’s digital ecosystem.

It becomes evident that the sporadic investments and developments that the State has granted to the eID field in the past are not in correlation with the responsibility the State bears in front of the end-users: the citizen and the State itself. The State’s dependency on the digital ecosystem must be accordingly acknowledged and backed up by financial means and moreover, by political reponsibility.

At the onset of the ROCA case, the State did not have an overview of its vast dependency on the eID. The existing risk assessments were unrealistic in respect of how big a threat the security flaw in the ID-card would pose to the State’s economy, essential public services and to the country’s overall digital ecosystem.

Therefore, *the primary responsibility for the State is to upkeep and guarantee the security of the eID.*

As demonstrated by the ROCA case, this responsibility can be elaborated into the following tasks:

a) *Continuous political steering and oversight*

- The eID area needs consolidated planning, management, and financing by the State. The ROCA case reveals that the lack of oversight of the eID area developments reaches a level of unintentional negligence. The amount of resources and attention dedicated to the field are so insufficient that consolidated management, development, and financing are entirely missing.

- The eID area needs a comprehensive policy for the eID management. As a reaction to the ROCA case, an initiative “*Identity Management 10-year Vision”* was launched by the PPA, the RIA and the MKM. Political steering is needed to ensure that the interests of all stakeholders are taken into consideration while creating a forward-looking political vision for the eID area.

- The State’s dependency on the digital ecosystem must be acknowledged and documented. The eID area needs a comprehensive map of public services and institutions that are dependent on the eID. The ROCA case helped the Estonian State to realize that such overview was missing, yet highly necessary for taking informed and timely decisions.

- The eID area needs sufficient human resources dedicated to it. The ROCA case revealed that the lack of experts and their time are the prime reasons for the above described undermanagement of this area.

b) *Determining the roles and responsibilities of all stakeholders involved in the eID area.*

- The eID area needs a leading institution to be assigned to steer and oversee the fulfilment of the given political guidelines. This leading institution needs to have the necessary (human, fiancial, political) resources in its disposal. The ROCA case revealed that there is no leading State institution with complete oversight nor responsibility over the eID area. The ROCA case also demonstrated that the RIA which was the State institution which *de facto* took the role of the leading institution in crisis management, did not have a clear political mandate for stepping into this role.

- The roles and responsibilities of different stakeholders to be determined and legally established. The ROCA case revealed that the legal responsibilities between public and private stakeholders are unclear, e.g. which organisation acts as the ETO in the eID area.

- It is necessary that the differences in organisational culture and operative models of the different State institutions that are involved in the eID area, are overcome. The ROCA case uncovered a serious mismatch between the operational conduct of different State bodies that carry shared responsibility for the eID area.

c) *Provision of security and durability of the eID service*

- The eID area needs increased cooperation between all stakoholders to guarantee the security of the eID service. The ROCA case illustrated how inter-dependent are the stakeholders in the Estonian eID area. An input from every stakeholder was required to continue offering the eID service in a secure and uninterrupted manner.

- The eID area needs sufficient financial and human resources to be dedicated to it. The ROCA case demonstrated that the lack of such investments leads to underlying security concerns.

- The eID area needs diversified circle of service providers in order to avoid dependencies on only one external service provider for its developments in the eID area. The conclusions made after the ROCA case lead to the realisation that there are elements in the eID supply chain that are considered as single point of failure and thus a security concern to be resolved.

- The eID area needs holding excercises on as practical level as possible while including all stakeholders to allow practicing inter-organisational crisis management. The ROCA case proved to be very similar to a scenario of an earlier exercise which was not taken seriously by the participants and failed to bring about substatial rise in awareness.

d) *Reviewing operational management models and crisis management guidelines*

- An inter-agency operative management model is required to be able to adequately address both the daily operations as well as crisis management in the eID area. The ROCA case revealed that until the responsibility for the eID area is scattered between different institutions, agency-centric management models, which were in use in 2017, are not sufficient.

- Including a response to a “non-incident” or a “risk” in the current eID area crisis management guidelines. The crisis management plans that were valid at the time of the ROCA case were not equipped to respond “non-incidents” such as the ROCA case. The interviews reveal that informal crisis management guidelines were worked out as the ROCA case was solved. Such guidelines need to be transferred into a legally valid form.

- The standard operational procedures in the eID area need to be reviewed considering the flexibility and informality of the “Estonian cooperation model”. The ROCA case demonstrated that an informal approach to the crisis resolution can be very effective in resolving a large-scale security risk in a small organisation. The values and attitudes prevalent in a given organisation determine the course of action and success with equal impact as the set formal procedural rules. This is a lesson the whole Estonian public sector should analyse and take into account. Further research on this topic may be necessary for developing a theory and respective public sector management model, taking into account the possible security risks and conflicts of interests.

5 Market and the EU

This chapter is divided into three sub-topics: Market, External Partners, and International Legal Regulation. Each sub-topic summarises a number of codes that originate from the thematic analysis.

5.1 Market

This sub-topic summarises the thematic analysis codes that relate to the European market for ICT products and services.

The European market for Trust Services is primarily regulated by the eIDAS regulation and in terms of identity management also influenced by the European Cybersecurity Act. In the EU, the Member States and private sector companies are competitors in providing the Trust Services including the provision of eID schemas.

5.1.1 Market influences

The full entry into force of the eIDAS's regulation in 2018 was a step towards enlivening the EU-wide Trust Service market. This forces the Estonian State to heighten its awareness of all the elements of its e-ID supply chain in order to be able to procure the necessary products and services at the best prices and conditions while acting as a service provider in its own right. Currently, Estonia is developing many State-ICT solutions itself. These are tailor-made developments are meet the country's specific needs, yet, are not as cost effective as the broadly used commercial solutions offered by larger ICT corporations. *"Because of the Estonian market size, we have 2 options: to either develop it ourselves (very specific; a lot of these solutions) or depend on big multinational corporations. For both of these you have to know the risks and* *own those risks as a service owner. It's not enough to map the dependencies and risks, that is a formality, you have to own them, management decisions have to be informed."*

The Estonian State is in a challenging role as a client for ICT services on the international market. With a population of 1.3 million people, catering for the needs of the small Estonian market with its tailor-made solutions does not pay off for the international service providers (primarily concerning ID-card certification and personification). For example, this is mentioned as the reason behind the high certification prices in Estonia compared with other countries. *"They can't deal with our ecosystem. The market is so small, so it does not pay off. If we look at certificates price here and in Europe, then we pay a very high price here."*

The State is moving away from developing all the solutions by itself and is now procuring the ID-card as a ready-made product from the international market. Some interviewees see this as a step backwards as the State loses control over the detailed build-up of the ID-card. However, others suggest that this minimises unnecessary work for the State and allows the State to concentrate on maintenance and testing the products it procures. Despite that the card production and personification were reported as tasks that the State is able to do itself, the certification is much more complicated and pricey service to provide. As mentioned above, the service providers are more interested in providing a full product rather than developing a custom-made or partial solution for the Estonian State. *"Ideally, RIA would be a regulator. Someone who synchronizes, solves disagreements, does not develop. Development is done because someone has to do it."*

With this in mind, the Estonian State has closed a new contract for acquiring the ID-card as fully certified product. To mitigate risks related to security and confidentiality, the new contract involves contractual penalties that were not in place before, applicable on the occasion of revoking certificates or malfunction of the chip. From security perspective, the State now believes that with the mID and SmartID[1] enabled, it has enough alternative authentication solutions available and relies on the contractual tools in case security flaws should occur.

[1] As of November 2018

It was suggested by the interviewees that the interests of larger European countries, such as the German and French, are better represented on the European market because the biggest certification centres are located in these countries. Also, bigger companies are better placed in terms of information and connections. It was inferred from the interviews that bigger customers – i.e. global corporations such as Google – seemed to have known about the fault in the chip encryption much earlier than Estonia. It was thus suggested that Estonia is in a difficult position in finding out such information. Also, it was suggested that the information regarding the fault was kept in silence on purpose, until a patch would be ready. An agreement of such kind was considered as one possible reason why Estonia did not find out the necessary info earlier. *"So maybe it was kept silent for a reason, because if countries find out, they will not keep quiet. And then Estonia came out with it in September and the big firms were still quiet."*

Likewise, big international companies see Estonia as too small client for offering highly customer-centred service. This can be rationalised by comparing the gained revenue of the service provider with the resources they are able to dedicate to their client.

The international corporations are responding to a small State's interest mildly, despite the political contacts involved in the communication chain. *"During the crisis, we saw, that we cannot realise support in Safari and Chrome, since Apple interface had a bug, it didn't support the elliptic curves. We escalated it to politicians, and they could start rising these questions. From Google after a month or so someone contacted, and it started moving; Apple just said, "thank you for letting us know".*

5.1.2 Public-private conflict of interests

The Estonian ID-card is unique in the world by its functions and scope. There are few similar products offered on the international market because there is no demand for it in a comparable format. Therefore, the specific needs of the Estonian State do not always overlap with the common products on the market. This concerns the build-up of the Estonian ID-card where the certification provider has access to highly sensitive private data about the card end-users while the chip and the card producers need to ensure the durability of the ID-card which the Estonian State and society are highly dependent on.

Therefore, Estonia is in a unique position as a State. Few other European countries present a similar e-ID model, yet no other country is as reliant on the State-provided digital ID as Estonia. *"It is an unknown land. Other countries do not have problems like this. They have a stronger private sector, because the firms are bigger, but we have a strong State side."*

There is a clear clash between the private sector business interests and the State's responsibility to guarantee service quality, security, and uninterrupted availability. Overall, the State benefits a lot more form private sector software and hardware developments than of those it is capable of providing itself. At the same time, the State is influenced by the business interests of those private sector companies and has to give up a certain amount of control and confidentiality by consuming the private sector services and products. This dynamic is also visible in the case of the Estonian ID-card. The composition of the Estonian ID-card relies on four different partners, two of which are public sector entities ant the remaining two are private sector companies. *"We are on 4 'legs': RIA, PPA, the developer, certification centres."*

In Estonia, the private sector companies are in the position of a Vital Service Provider (ETO) that are regulated in the Emergency Law and thus bear higher responsibility towards the durability and security of the services they provide. The conflict of interests emerges as the State has a duty to regulate this field and be more aware of the technical background of these companies (or even have access to their information in certain cases), while on the other hand, the State cannot interfere with the business interests of these companies. *"No…. Many of the Vital Service providers are private companies and how to go on check their systems as a State…? Is it legally even possible? The private sector has its trade secrets' protection in effect. So how can the State protect their secrets, when we might have full access to it?"*

Moreover, appropriate domestic legal instruments must be developed to support the State in this role. Lack of appropriate legal instruments are partly to blame for the failed cooperation with Gemalto. It is hoped that these measures would place more responsibility for similar failures as the ROCA vulnerability, on the card producer. The international reputation of the ID-card and the microchip producer is another element that forces the companies to guarantee the quality of its products.

It was also underlined that by updating its legal framework, the State would gain a better negotiating position with the private sector service providers in terms of prices. With stronger competition, the prices would become more favourable for the State. *"With the last procurement, we had a momentary competition situation that showed how prices dropped instantly."*

It was questioned on which level legal regulation would be the most appropriate for dealing with international private companies: domestic or international? It was suggested that the requirements for the regulations vary: different legal instruments may be needed for crisis situations and for dealing with international partners.

The interviews revealed that the private sector company Gemalto (Trüb) drove the Estonian ID-card development for a number of years. The reason being that the development had not been assigned to a certain Estonian State institution but fell between the areas of responsibilities of different State bodies. With this, Gemalto (Trüb) was in a position where it could easily steer the ID-card technical developments based on their best interests. *"In 2013 we started to realize that the development of the ID-card was not dictated by the state but a private company: Trüb. This was because the PPA is not an IT-institution, this competence left in 2009 to the SMIT (IT and Development Centre in the Interior Ministry) and the competence about the ID-card was left somewhere – because the PPA nor the SMIT took it on board."*

It appears that there has been a lack of understanding about what it takes to up-keep the State ICT developments in order to keep them modern and secure. Up until 2014, the State was acting on an autopilot, its eID contractual and technical aspects were underdeveloped and based on outdated information. Given this, the contract that was signed with Gemalto in 2010 was likely to be unfavourable for the Estonian State. *"When I got this area to work with (in the end of 2014), then time had stopped. ... The state was in a complete comfort-zone."*

It emerges that there was a lack of transparency in the communication with the Gemalto. The ROCA case finally directed the State to analyse its cooperation with that company in closer detail. Severe deficiencies in cooperation and service provision were revealed and thus, the cooperation between the two sides ended. The disagreements that emerged from the case were brought to court. The code “Gemalto (Trüb)” analyses this topic in greater detail.

Public and private interests collided also regarding the formal notification procedures for security risks, i.e. the ROCA vulnerability. The State has a responsibility to provide transparency and public service quality. It appeared that private sector business interests very likely collided with that. The IT security specialists find that releasing information about a vulnerability before a possible fix has been developed, constitutes a considerable security concern. This is one way to explain why the service provider was not interested in wider knowledge about the ROCA vulnerability and thus, Estonia was not duly and timely notified. *“The problem is that states make this info public. It is in no-one’s interest to make things public before big companies have the patches.”*

However, for the Estonian State with its entire digital ecosystem, the knowledge about the ROCA vulnerability was of fundamental importance. It is not hard to imagine how damaging it would have been to Estonia's image as a trustworthy e-State and a pioneer in internet voting – domestically and internationally – if just one card’s encryption would have been broken. *“Two formal means of notifying let us down. Partly because they are built for a crisis, not risks, partly because Estonia is just such a small client.”*

5.1.3 Public-private cooperation: “The Estonian cooperation model”

The private sector is a partner of crucial importance for the Estonian State. As outlined above, the ID-card development has come forth with a significant contribution from the private companies. The same is true for the overall functioning of the Estonian digital ecosystem and how the electronic authentication has been taken into use. Undeniable partners are the banks and telecom companies that are most intensely both benefitting from and promoting the electronic authentication in all available forms in Estonia. Those private sector entities are also enjoying a special treatment by the State. As an example of that: the banks were informed prior the public about the ROCA vulnerability. Similarly, any strategic planning by the State side cannot be successfully done without including the influences and perspectives originating from the private sector stakeholders.

The public-private cooperation during the ROCA case was exceptionally helpful towards the State. A number of public and private sector stakeholders offered the State its help and were willing to contribute without direct involvement of business interests and the individual experts offered voluntary input. *"All IT companies, who were connected somehow, offered their help. No one asked if we're paying for it or not, about a contract or anything." "You also offered help (TTÜ), the banks. Basically, take what you need!"*

Despite the State's dependency on its certification provider SK Identity Solutions AS, the cooperation with SK is seen as excellent and trusting. *"During this case, very good, they were working with us. Business interests didn't show." The right people with the right values? "Exactly."*

It is visible form the above statements that the attitude and prevalent work ethics in a given organisation plays equally important role as the institutional hierarchy and formally established workflows. The ROCA case demonstrated that the people involved in crisis management guaranteed the success of the solving of the case. It can be inferred from the interviews that these people carried common values towards their work and the State, irrespective if they represented a private or public sector stakeholder. This aspect was described as the "the Estonian cooperation model" in the interviews. *"Cooperation can be done a lot less effectively: the PPA could've written a letter to the RIA, 30 days answering time for RIA… etc." "No law is going to help us solve any crisis, every situation is different, and people do the solving. Not institutions' roles or plans, but people"*

5.2 External Partners

This sub-topic provides an analysis of the codes describing Estonia's private-sector partners in the eID supply chain.

5.2.1 Gemalto (Trüb)

Cooperation with Gemalto throughout the ROCA case has varied. In the early stages when it was still unclear how far-reaching consequences the flaw in encryption would pose for Estonia, Gemalto's cooperation with the Estonian authorities regarding the technical details was rated positively. The technical process of renewing the certificates was carried out in cooperation with Gemalto. Later on, as the Estonian authorities gained an impression that the private sector firm had been withholding information from Estonia, the cooperation froze. Estonia presented charges against the company and the communication and cooperation stalled after the court case was launched.

It can be inferred from the interviews that Gemalto did have a contractual responsibility to fix the fault in the ID-card for Estonia. However, Estonia did not trust the partner enough to wait for a solution initiated by Gemalto.

One of the core aspects of the disagreement between Gemalto and the Estonian State was said to be insufficient information exchange regarding the ROCA vulnerability. Gemalto claims that the information regarding the faulty chips had been passed on to the Estonian authorities on the right time. Estonian authorities claim that this is not true. According to the interviewees, the chip producer, Infenion, informed its clients in February 2017. Estonia received official information form Gemalto on August 31 the same year. No explanation was presented why the time lag between the two notifications was so long. It was inferred several times in the interviews that the chip and card producers likely did not want the information regarding the fault to spread. There were various speculations regarding the reasons for that. *"Infineon makes the chip, Gemalto uses it. In Estonia Gemalto/Trüb personifies it and prints the visual image on the card." "A big corporation thought of us as a small part and did not see the need to inform us. They didn't understand our dependency."*

It can be inferred that Gemalto's decision not to inform Estonia of the faulty chip may have given the company a setback in form of reputation and credibility loss in the eyes of its international partners and competitors. Not only did the company make a severe underestimation of the importance of the ID-card for Estonia but also in terms of Estonia's image on the international market. Estonia as a client is seen insignificant in financial return, but an important client for presenting a certain image on the information and communication technologies market. *"One thing that influences the* *producer is Estonian reputation. Document producers are very interested in getting a contract with us." "If Estonia decides that they have violated the contracts, then they could be disqualified from all procurements from Europe. There is much money in those."*

As the manufacturer of the ID-card, Gemalto (Trüb) has had a strong influence on the technical development of the Estonian ID-card. On part of the Estonian State, the cooperation with the card provider had not been thought through for several years. Partly, this is because the State has been lacking consistency in terms of personnel overseeing this project. Another reason was insufficient technological competence in the overseeing State institution. It was described by the interviewees that the technical competence was moved away from the Police and Border Guard in 2009. After that, this competence and responsibility should have been taken up by the Interior Ministry. However, this did not happen. As of necessity, the technological competence and oversight of the ID-card became the responsibility of the Information Systems Authority (RIA). *"On our side (the State) people have changed a lot, there hasn't been consistency. Our partner has had the same people during all this time. During every 'crisis' there have been new people on our side."*

It can be inferred from the interviews that until 2015 the State had no clear overview of the ID-card provision. Gemalto (Trüb) as service provider was never audited by the Estonian State. The final audit was ordered by the PPA only by the termination of the contract in 2017. *"Up until 2015 there were no audits because people were in a comfort-zone. They trusted the partner, that they will do their usual audits. ... This wasn't a priority."*

Third reason for an unfavourable cooperation conditions with Gemalto (Trüb) was a gap in Estonian legal regulation. The production of the ID-card had not been defined as a supporting service to the Vital Service (ID-card) and therefore no other legal requirements were applicable except for the contractual agreements between the parties. *"Service agreement with private companies is missing concerning the rights, obligations, and processes with the certification centre. We have no idea, what Trüb/Gemalto were doing, we haven't seen any logs or anything."*

With this, it can be concluded that the ID-card project – a Vital Service for the State and a fundamental element of the whole Estonian e-State - has been significantly undermanaged by the State for several years. Likewise, the eID area has been underrated in terms of financial and human resources.

5.2.2 SK Identity Solutions AS

At the time of the 2017 ROCA case, Estonia was found in a situation where there was only one Estonian-based ID-card certification provider, the SK Identity Solutions AS. The State is the most worried about its vast dependency on this certification provider. Should this company face any unexpected difficulties, the Estonian State would not have an alternative service provider for certification. *"I actually fear more the dependence on the certification service provider. Also, in the new contract we cannot do without them, we tried to liven up the market with this procurement, but it didn't work out."*

Moreover, the monopolist status of this company is another reason for the certification prices to remain high in Estonia. Developing State regulations to enliven the competition in this sphere was mentioned as one option for improving the situation by the interviewees. Acquiring State shares in the company providing the certification service providing was suggested as another solution.

There is lack of clarity regarding the roles and responsibilities of the different institutions involved in the provision of the Estonian ID-card. This raised a number of questions among the involved parties while working on finding the resolution to the ROCA vulnerability. From legal perspective, the role of the Vital Service Provider, and the responsibilities resulting from that, is not fully specified. Different interpretations allow calling both the SK and the PPA a Vital Service Provider (ETO).

Despite that the in Estonian Emergency Law (HOS) stipulates that the identity document is issued by the same authority as the certificates, which makes the PPA the Vital Service Provider, the PPA disagrees with such a classification. Instead, it suggests that the SK, who is the actual certification provider, is also the ETO who is acting on PPA's behalf.

5.2.3 ICT community

The interviewees noted a need for creating a wider ICT community which would involve experts with different backgrounds: developers, analysts, IT-managers, academia. Both, public and private sector experts should be involved, importantly including those who have transferred their careers from one sector to another to improve the transfer of knowledge and competences across the ICT field. This circle of people would likely to be the holders of key expertise and act as opinion-leaders. Having this kind information sharing network would speed up the information exchange in crisis situations and facilitate information sharing and best practices on regular basis. In this context, the interest was to widen the circle of people who are particularly aware of the developments in the field of electronic identification and authentication. *"The State should have more collaborative partners. In this field there's a lot of expertise that is just communication based, but if you leave, you take all your contacts with you as well. So, it would help to have a working partner network, so you'd know who works with what."*

The State would also benefit from such a network for finding the right kind of expertise and contacts when the need arises. The eID Coordination Council, summoned by the RIA, was mentioned as a good basis for forming such a network. *"I think we shouldn't have a lot of people working for the State but have a capability to buy the competences from the universities, the state doesn't have to know everything, but we have to know how to get it."*

Importantly, it was emphasised that a strong IT-community could serve to inspire more people to study ICT in universities to help to lower the deficit of qualified experts in the IT field.

5.3 International Legal Regulation

This sub-topic summarises the thematic analysis codes that describe different aspects of the international legal framework applicable to electronic identity provision and is relevant in the 2017 ROCA case context.

5.3.1 The eIDAS and Estonian domestic legislation

The interviewees voiced the opinion that the Estonian eIDAS implementation acts (these regulate the issuance and certification of electronic authentication and signature devices as well as the suspension of these certificates) are unnecessarily detailed – trying to name all types of incidents which would result in revocation of the certificates of the Estonian ID-card. It was proposed that instead of determining each possible incident type in legislation, it would be more useful to determine on which political level the decisions regarding the revocation of the certificates is made. It should be taken into account what services and which users are affected and what effect would the escalation of the situation bring. Informing all stakeholders is considered vital.

It was believed that in case of a large-scale security risk, the final decision regarding the revocation of ID-card certificates is always at the hands of the country's political leadership. This is because such suspension of the electronic authentication and signature tool has potential economic and political effect, which depth may vary depending on the country. *"In cases that big, the decisions are not made by lawyers or technicians, but by politicians. I think we are trying to be too detailed in legislations and regulate in advance."*

At the early stages of the ROCA case, some interviewees believed that giving a notification about the security flaw on the ID-card chip following the rules set up in the eIDAS, would have initiated an immediate revocation of the Estonian ID-card certificates. It was feared that this would have rendered the affected 740 000 cards digitally useless or resulted in removing the Estonian eID from the EU Trusted List. Such a scenario would have had a devastating effect on a country like Estonia that is heavily dependent on its electronic authentication mechanism in its every-day functions.

A legal analysis conducted by the Estonian State suggests that such a scenario could not have realised, and that the EU incident notification process is merely of informative nature and aims at informing other potentially affected parties. *"Deleting from any qualified Trust Service list could not have happened."*

A contradiction can be found in the Estonian legal framework between the eIDAS and an earlier domestic legislation. Before the adoption of the eIDAS, Estonia has been using its own Identity Documents Act (ITDS) as well as the Electronic Identification and Trust Services for Electronic Transactions Act (EUTS) for regulating the use of the ID-card. With the entry into force of the eIDAS, there are three laws regulating the same subject in Estonia. Despite a domestic agreement on how these laws should be treated in relation to one another, a more thorough review with possible amendments is needed. *"We have an agreement how they should be taken into action, but there may be collisions or contradictions. In practice, there are not problems, but formally maybe."*

While there has been criticism regarding the eIDAS being too unspecific in terms of procedures, another view presented in the interviews recognises the eIDAS as a general framework, finding it positive that the Member States have been left with certain freedom in implementation.

5.3.2 The eIDAS and international cooperation

The ROCA case was solved by using an elliptic curve cryptography (ECC) to replace the RSA library on the ID-card microchips. Compliance with the legal framework was one of the reasons for this decision. If Estonia would have proposed an entirely new authentication mechanism, it would have had to undergo the European certification mechanism. This was considered too time consuming and therefore an update to the existing ID-card chip had to be considered. Moreover, a significant number of ID-cards was unaffected by the faulty chips and did not need to be replaced. *"There is a part of cards, that are vulnerable, but we still have a bunch of cards that aren't threatened, so we have to make changes in a way that doesn't kill the whole ecosystem."*

The interviewees strongly underlined that the certification mechanism under the eIDAS is overly time consuming. In a situation, when a new product needs the certification to be granted in order to replace an outdated or insecure product, the long-lasting certification process in fact reduces security. An example was the Estonian SmartID that could have been used as an alternative authentication tool to the ID-card in Estonia soon after the announcement of the ROCA vulnerability. That way, the potential revocation of 740 000 ID-card certificates would have had lesser effect. Thus, the interviewees wonder what is the real effect – or aim – of the eIDAS is. As some view it, the European cybersecurity certification framework poses a market barrier. *"Certifying has multiple aims: ensuring security, market control, because certifying is actually just market barrier and a process for raising mutual trust. The EU should think what the eIDAS certification is for, where it is preventing actual security etc."*

It was also stated by the interviewees that the trust framework, the European cybersecurity certification framework, does little to actually provide security and trust among the Member States. A comparison was made with the SOG-is[1] framework where 17 European Union countries aim to cooperate towards harmonising security certification and coordinate the development of protection profiles in relation to any new IT-security directives put forward by the European Commission (SOG-is, 2019). Within the SOG-is framework, the member countries regularly audit each other's certification mechanisms. This practice familiarises the members with each-others' certification processes and common standards are thus formed. None of this is true for the eIDAS central certification mechanism under which the knowledge regarding other countries' certification products is restricted. *"It was surprising (during the ID-crisis), that in essence, we can do anything as a country. When we said, we will change this and do that, no one cared! During the crisis nor afterwards, no one has asked, what we did in terms of technical aspects. In the SOG-is scheme there would have been questions on how the update was made, who checked it, who tested it, who are the competent specialists. In eIDAS this is a question within every country, how the certification processes are built. This can't build trust in Europe."*

[1] The SOG-IS agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria. The agreement was updated in January 2010.

It is suggested by the interviewees that the eIDAS interferes with the State's autonomy in issuing their electronic identity documents. The reasoning is the following: in a situation where the technologies enabling the State eID should malfunction, it is the State that bears the responsibility for the potential losses, not the producer of the technology. It is likely that the State may have to cease offering the eID service, which, potentially, has an immense effect on the day-to-day functioning of the society. *"eIDAS is overregulated: certification is one lab, then by BSI, then Anssi, and actually there is nothing that protects us. What is it for then?"*

Moreover, the State has the responsibility to guarantee the authenticity of an e-Signature and the validity of a digital ID. The argumentation draws a parallel with the national passport – countries trust each other's passports. Why cannot they trust each other's digital identities? The State carries and unprecedented responsibility in terms of digital identity verification. Handwritten signatures as well as passports are verified and proofed via different, low-tech, procedures as compared to verifying the authenticity of a digital signature. *"The State takes the responsibility. If we make a mistake and someone forges our signature, then the State will guarantee some legal link there. Do we need certification? On transnational basis, we acknowledge passports, if they satisfy the requirements, but they are not certified. With the digital signature we need certification. It is the State's responsibility, our playground, we trust this. The same goes for the State's eID schemes. With eIDAS we will start writing peer-reviews on if we trust German ID-card. What right do we have to say we do not? We trust their passports."*

The interviewees reveal that on the EU level, Estonia seeks allies to bring forward an initiative for changing the current European cybersecurity certification framework. This proposal would foresee placing the responsibility for guaranteeing the integrity and security of the eID and e-Signature to the country offering that digital solution. This would cease the overseeing powers of the central certification authority. At present, this central certification authority can only issue a stamp of trustworthiness, but it has no means to enforce the guarantee that the certified product remains secure and uncorrupted. It can only be the document issuing State who can guarantee the trustworthiness of its eID and take measures in case its eID is misused.

5.3.3 Notification

Two formal notification mechanisms exist in Europe for giving notification about security flaws and incidents. These are the formal notification by the technology producer and the formal incident notification by the European Union Member States. Neither of these notification mechanisms were successful in spreading the information regarding the ROCA vulnerability on the Infenion chips. The vulnerability was discovered by Czech mathematicians who informed the chip producer in February 2017. *"The two formal means of notifying let us down. Partly because they are built for a crisis, not risks, partly because Estonia is just such a small client."*

This information had not reached Estonia in a meaningful way via official channels by August 2017. The true information reached the RIA via informal contacts, by a notification made by the Czech academics who discovered the ROCA vulnerability. Despite the contact was at first established via informal channels, the duly composed notification then reached the appropriate channels without a delay. *"It is good, that RIA has these connections, and they got the info from the Czechs thanks to personal contacts, which isn't the usual track."*

Why wasn't Estonia duly notified by the chip producer? Two scenarios emerge: first, Estonia was seen as a small and unimportant client whose dependency on the ID-card was not known to the chip producer. Second, the information was intentionally kept secret from Estonia because publishing it before a patch was ready would have increased the security risk as well as caused reputation and credibility loss for the chip producer (Infenion).

The whole Estonian e-ecosystem was put in risk due to insufficient notification. The Estonian authorities would have benefitted from earlier notification as the timeframe for getting the fault fixed was very short: an alternative solution had to be worked out before the academic work related to the discovery of the flaw was going to be published (October 30, 2017). An earlier notification would have allowed more time for working out the solution for Estonia and the transition to new certificates could have been smoother. Due to time constraint, the certificate renewal was launched without testing and this caused hardships during the certificate renewal process. Importantly, this way, the related security risks would have played a smaller role. *"The e-services would have had more time for transitions and their own developments, citizens would have had* *more time. The suspension of certificates was connected to publicizing the academic work."*

As a result, Estonian State has presented claims against Gemalto (Trüb) for withholding information about the faulty encryption on the chip used in the Estonian ID-cards. It was stated in the interviews that the chip manufacturer was informed about the ROCA vulnerability in February 2017, while an official notification by Infenion was made in May 2017. Curiously, it was alleged by the interviewees that Infenion's global corporate clients, such as Google, were already changing their cards at the same time, in May 2017. The Infenion representative in Estonia denied even in June 2017 that the faults Austria had recently reported via European notification mechanism had anything to do with the chips used in Estonia. The opposite turned out to be true.

In Austria, a private-sector card with this faulty chip was affected by the ROCA vulnerability. A very generally worded notification about this incident was sent to the European Union Member States in summer 2019. Estonia and many other countries failed to pick up the necessary information from the Austrian notification. It was said to be very general and did not include detailed enough information for it to be considered relevant by the Estonian experts that processed this letter.

Resulting from the notification duty set up in the eIDAs, Estonia filed a notification to the European Union Member States after finding out about the ROCA vulnerability. A careful wording was chosen: reporting a threat rather than an incident. In the initial stage of the ROCA case it was unclear what effect notifying of the Estonian situation would have. The fear of revocation of the Estonian ID-card certificates turned out to be ungrounded, yet it created a significant discussion. Revoking the ID-card certificates would have meant for Estonia the cessation of the digital functions (authentication and digital Signature) of the ID-card. Reporting a threat allowed to inform the European partners while the digital functions of the ID card remained uninterrupted. The case was solved by offering the end users an opportunity for remote (online) renewal of the ID-card certificates.

ENISA rated the Estonian notification positively, saying it was detailed and technical. However, neither this notification was well understood by other EU countries that were affected by the faulty chips (Spain, Slovakia, and Poland). Thus, the European Union notification mechanism was found largely insufficient by the interviewees. The primary reason for the failure of the notification mechanism was that there was indeed no security incident. The risk posed by the ROCA vulnerability did not realise. There are no formal procedures established for notifying of a threat or a "non-incident" and the Member States had no better tools for reacting to this situation. *"The reality is that no one had considered a non-incident incident. Risk and vulnerability were not considered. There were no extra-resources. The European notification mechanisms, not to mention the Estonian ones, hadn't seen this as a possibility."*

5.3.4 Reacting to a "non-incident"

Classifying the ROCA case was a difficult question for the interviewees. Not one ID-card's encryption was broken, incident did not happen. However, the threat was imminent and required immediate action. Neither the eIDAs nor the Estonian domestic legislation offer suitable legal tools for addressing a situation that is not an incident, but a threat or a risk. The Estonian HOS allows to classify a situation as a threat of an emergency. However, as the HOS does not establish any extra tools for responding to such a situation, there is no difference in how the situation is classified unless it is an emergency or a clearly definable incident.

The interviewees stated that calling a state of emergency would not have given the State any noticeable added value while solving the situation. All stakeholders cooperated and offered their help according to their best capability, all actions already were on optimal level. *"The objective need for announcing an emergency was absent. The new HOLP (plan for solving emergencies) was enforced, digital signing is a Vital Service."*

It was suggested in the interviews that the existing legal tools must be adjusted also for this kind of situations. The aim of the law-making is to give the State general frameworks for handling any kind of threat by the most optimal means. Adding technical, software- or hardware-based details into legislation is likely to prove counterproductive. The technology evolves rapidly, and it is therefore challenging to comprehensively foresee all possible types of threats. *"If we have a leadership model for a crisis situation, then it doesn't make sense to make a different one for not-exactly-*

a-crisis, it would make sense to take a limited model from the crisis model and bring it to peace-time."

The difficulty in handling a non-incident of such scale is that there are no formal rules of conduct: no formal rules regarding which institution takes the lead and is responsible for the decisions taken. It is especially complex in Estonia's case as there are several institutions that have a certain responsibility for the e-ID service, all competences and tasks are not under the responsibility of a one single institution.

The RIA was the leading organisation for resolving the case in Estonia. The RIA was considered having the biggest amount of expertise and manpower to handle such a situation. Considering the severity of the potential outcomes, if the risk of breaking the encryption of the ID-card would have realised, it was often discussed if RIA truly had the mandate to lead the crisis management. *"At some point we discussed in our management if RIA is the right place to lead this and we decided that it was. We have different areas we are responsible for."*

The interviewees mentioned training and exercises as suitable tools for increasing preparedness for combating similar non-emergency situations in the future.

5.4 Conclusions of theme "Market and the EU"

This section provides an answer to the sub-research question: Which roles for the information and communication technologies industry emerge from the case?

Estonian ID-card is unique in the world by its functions and scope**.** Few other European countries present a similar e-ID model, yet no other country is as reliant on the State-provided digital identity document as Estonia. This puts Estonia into a unique position in the European Union.

The Theme 2 "Market and the EU" reveals that the Estonian State has an unprecedented responsibility in terms of digital identity verification. While considering conventional identity documents such as national passports and ID-cards, the responsibility to ensure the security and authenticity of these documents lies entirely on the State issuing these documents. In the digital realm, the European Union has the oversight as stipulated in the eIDAS regulation. It was suggested in the interviews that the eIDAS regulation in fact interferes with the State's autonomy in issuing their electronic identity documents. Likewise, it was suggested by the interviewees that the European cybersecurity certification framework does little to actually provide security and trust among the EU Member States.

On the harmonised European Union Trust Services market, the Estonian State acts as a service provider and as a client for ICT solutions (hardware and software alike). The latter role is a challenging for Estonia. Often, catering for the needs of small Estonian market with its tailor-made solutions does not pay off for the international service providers. Likewise, Estonia is in a difficult position for finding out information about security flaws and receiving customer-centred service from service providers for whom Estonia comes across as an insignificant source of profit.

It appears that there is a clear clash between the private sector business interests and the State's responsibility to guarantee service quality, security, and uninterrupted availability.

Both, the incident notification by the European Union Member States and by the technology producer, failed at spreading the information regarding the ROCA vulnerability on the chips used on the Estonian ID-card. The interviewees found the European Union notification mechanism largely insufficient. The whole Estonian e-ecosystem was put in risk as a result.

The Estonian State classified the ROCA vulnerability as a threat or a risk, not as an incident. The risk posed by the ROCA vulnerability did not realise, i.e. not one Estonian ID-card's encryption was broken, no incident occurred. Neither the eIDAs nor the Estonian domestic legislation offer suitable legal tools for addressing such a "non-incident".

The different stakeholders of the ICT industry are represented in a number of roles in the ROCA case:

- *Private sector service providers act as Vital Service providers* to the Estonian State. The ROCA case demonstrated that the private sector certification provider fills the role of a Vital Service Provider on behalf of the PPA. The Vital Service providers are regulated in the Estonian Emergency Law and thus bear higher responsibility towards the durability and security of the services they provide.

- *Private companies act as partners in public-private-partnerships and as service providers* to the State. While the State wins form purchasing its software solutions and other products from the private sector providers, the State is influenced by the business interests of those private sector companies and has to give up a certain amount of control and confidentiality by consuming the private sector services and products.

    - The banks and the telecom companies in Estonia act as undeniable partners to the Estonian State. These stakeholders are most intensely both benefitting from and promoting the electronic authentication in all available forms in Estonia.

    - The ID-card certification provider. The ROCA case revealed Estonia's vast dependency on its sole ID-card certification provider. This not only constitutes a security risk, but also results in high certification prices for the Estonian State.

    - The ID-card producer. The private sector business interests collided with the State's responsibility to guarantee service quality, security, and uninterrupted availability. It was suggested that the information regarding the ROCA vulnerability was intentionally kept in secrecy to protect the chip and the ID-card producers' business interests while setting the entire Estonian digital ecosystem at risk.

- *ICT community*. The ICT community is a circle of experts with formal and informal contacts with the Estonian State. The ICT community is seen as an information sharing network and a basis for the State to scale up its respective ICT capacities in crisis situations. The ROCA case demonstrated that international informal contacts within the ICT community played a key role in transmitting the information and by this surpassed the capabilities of the formal notification mechanisms. This allows to question the effectiveness of the formal notification mechanisms.

- *Academia.* The academia, in constant interaction with the ICT industry, plays a role in every stage of ICT services and products' development. In ROCA case, the academia played a key role in discovering the fault in encryption, in communication and publishing the info about the vulnerability to the industry and to external stakeholders. The academia also offered its help for crisis resolution purposes.

- *International regulation (1): eIDAS.* The eIDAS regulation harmonises the European Trust Services market (including the eID area), defines and sets the standards for the Trust Services, establishes the inter-State notification duty and procedures. In the ROCA case, the pan-European notification mechanism proved to be inefficient.

- *International regulation (2): The European Cyber Security Act, the international security frameworks SOG-is and European cybersecurity certification framework.* These frameworks can be in supporting or hindering role for the eID area and for eID security provision. The ROCA case brought about a recognition that the European cybersecurity certification framework poses a market barrier for new Trust Services and is inefficient in providing security and trust among the EU Member States.

- *The State as a customer for ICT products.* In this role, the State can act as a market influencer through the specifications of the products that it procures from the market. As a client, the State has the capacity to set the demand (resulting from the purchasing power of each particular State). In parallel with the ROCA case, the Estonian State changed the specifications to its new ID-card procurement. The interviewees also indicated that the specific needs of the Estonian State do not always overlap with the common products available on the European ICT market and this presents challenges for the State.

- *The State as ICT service provider.* The State is a contributor to the ICT industry – with expertise and (pioneering) eID solutions. The Estonian ID-card is unique in the world by its functions and scope of usage**.** Few other European countries present a similar e-ID model, yet no other country is as reliant on the State-provided digital ID as Estonia. This puts Estonia into a unique position as a State.

6 End User

This chapter presents the thematic analysis findings for the theme "End User" and is divided into two sub-sections: "Estonian e-ecosystem" and "Impact on the Information Society".

6.1 Estonian e-ecosystem

This sub-topic uncovers how the codes related to the Estonian digital ecosystem were discussed in the interviews and which topics emerged.

6.1.1 Digital ecosystem

The ROCA case indeed made clear that the eID is fundamental infrastructure for the every-day working of the private and the State sector. At the onset of the ROCA case in autumn 2017, the State was unaware of the depth and extent of its dependence on the eID. As the case evolved, it became rapidly clear that the dependencies within the private and public sector are manifold and significant. *"When the crisis started, we asked them to map the dependencies if all ID-cards are revoked and then panic started – everyone had dependencies. The actual effect appeared then."*

In addition, it became utterly clear that the State itself is the primary dependent end-user of the eID. *"One client was the citizen, but the others were the State functions."*

The interviewees mention that an exercise was carried out earlier in 2017 that was specially targeted at mapping the State services and institutions dependent on the ID-card. This initiative was unfruitful as only one institution reported having a mild dependency. It can be inferred from the interviews that the attempt to map the dependencies was too superficial: too general questions were asked, and not enough knowledgeable specialists were involved. In order to meaningfully analyse the dependencies on the eID, sufficient knowledge of the Estonian e-ecosystem is required from the person(s) conducting the research. *“There have been exercises with public sector institutions also, where for example we got information that there are no big dependencies on the ID-card. Later we found out that there were many. Some of them critical, e.g. there were not alternatives. We didn’t understand that ID-card infrastructure is basic infra, it affects the public and private sector both.”*

The true problem seems to be that the State does not have a clear definition of what constitutes a dependency. Is any service that is using the eID for authentication and digital signing dependent on the eID? In which extent does the public service have to be impaired at the event of the eID malfunction for it to be considered dependent on the eID? These were some of the questions that the interviewees raised. *„How low does the quality of a service have to go for it to stop?“ (CERT)*

Different opinions on how to map those dependencies were voiced throughout the interviews. Some of which were stating that it is impossible to map all the eID dependencies. The reasoning behind these opinions was that the Estonian e-ecosystem is so wide: the Estonian x-Road involves more than 3000 different services while the main enabler for connecting to these services is the eID, serving for digital authentication and signature alike. *“We are not able to map all dependencies. The next time it will turn out that the error is in the patch, then we need a list for that. Then the problem is in open ssl, then a new list. To have a list in the State, of all the dependencies and cross-dependencies, is hopeless.”*

Other interviewees made suggestions to follow the definition of the HOS, or simply pick a number of top critical services and limit the list in this manner. The x-Road has been suggested as another element that could be used as the basis for such mapping. However, it is important to notice the conflicting opinions presented in the interviews. *“Start with the data connection, ID-card, x-Road…max top10 things.” “We can’t map them all, just the important ones. Public services, those that fall under HOS.” “One way is to map critical functions, not only what HOS (Emergency Law) states, but wider. e-ID is in there, but x-Road is not. With x-Road it is easy – all that is in there, is dependent.”*

Furthermore, there are cross-dependencies that involve both, technological and organisational spectre.

The level of technical preparedness varies among different institutions. Parts of the e-ecosystem are unevenly prepared (for crisis, for technological updates etc.). Some institutions were able to rapidly react to the renewal of ID-card certificates, others were faced with technological challenges that slowed down the renewal process. In some cases, the institutions were forced to stop their daily functions as the updated certificates would not comply with their IT systems.

Not knowing the level of technological preparedness of all involved public institutions made the renewal of the ID-card certificates more difficult. *"When we knew about starting using elliptical curves algorithm, then quite many of them told us, that they won't be able to implement the new algorithm capability for the end of the year*."

Importantly, electronic voting is a democratic process that is dependent on the ID-card and electronic authentication in Estonia. The sub-topic "Impact on the Information Society" analyses this subject in greater detail.

6.1.2 eID User Groups

The interviews reveal that the total number of ID-cards affected by the ROCA vulnerability was close to 750 000. It became clear that not all these users were equally dependent on the electronic functions of their ID-cards[1]. The user behaviour of the card owners whose ID cards were affected by the ROCA vulnerability was described as follows: *"Almost 100 000 of them haven't ever used the e-services at all. But there are about 150 000-200 000 clients, whose life depends on it."*

The interviews further reveal that this severe difference in user-behaviour among the ID-card users was not acknowledged well enough by the authorities prior to the crisis[2].

[1] The Estonian ID-card serves as a valid travel and identification document regardless of the status of its electronic functions and the status of its certificates, respective to the ROCA vulnerability.

The need for better knowledge about the user-groups and user behaviour was stated repeatedly by the interviewees.

Not being aware of how, in which extent and by whom the ID-cards are used, hindered the State from taking the most optimal counter measures to mitigate the crisis. Knowing the user-groups would have provided a technological and tactical leverage (i.e. targeting smaller user groups at a time and in prioritised order to avoid overhauling the system). *"Not understanding who the dependent user groups were, caused hardships with the renewal of the certificates."*

The ROCA vulnerability demonstrated that the misinformed end-users that rarely use the ID-card electronically, flocked to the PPA service stations and overcrowded the service stations. This cut off those end-users who needed the ID-card critically for carrying out their public functions of business activity from getting the assistance they needed to renew their certificates. Better targeted communication by the State would have helped to avoid such a scenario from unfolding. *"User profiles. We need it in our services, but especially during a crisis. Then we'd know how to communicate messages."*

The information was missing regarding the most active users and most impactful users (referred to as the "power-users" i.e. the notaries, the doctors, judiciary, the Government). This made the crisis resolution more cumbersome. A suggestion to compile a list of vital State functions was made by the interviewees. It was argued that segmenting the users by their public functions and the frequency of electronic use of their ID-cards could give the State a better chance to guarantee the security of the e-authentication service offered via the ID-card. *"There should be a list of work positions. Then in this crisis we wouldn't have had to solve it through people but through institutions."*

It was suggested that in a crisis situation, when the overall functioning of the society is at stake, the most vital functions and most active users should be prioritised by using segmented communication. While some interviewees were strongly in favour of such solution, some others did not see added value in this. *"They didn't understand the need for it. The target group was 750 000 and unnecessary panic was induced in many people. If the crisis involves masses, then target groups should be defined."*

On the other hand, the principle of equality was also stressed: *"The State issues documents to everybody, it doesn't matter how much you use it. So, in this sense we have to treat everyone equally."* During the remote renewal process, there were attempts to prioritise certain users, however, these attempts failed due to technical difficulties.

Another principal idea that was presented in the interviews was prioritizing State functions over the private end user's needs at the event of a crisis. The State is both, the primary provider, and the primary end user of the Estonian digital infrastructure within the e-ecosystem. At the event of a crisis and given limited resources, the State's priority should be guaranteeing the functioning and seamless provision of the public services ahead of the individual citizen's needs. *"We have to have a plan of action for when something breaks. Maybe a citizen, who has the ID-card, will have some trouble, but the State would survive."* Resulting from the crisis, it was proposed that the State would benefit from providing the State officiates with an official ID-card, a separate identification and authentication means intended for professional use only. The professional eID would provide better overview of the vitally critical State functions and allow accessing this this type of user data without the violation of personal privacy.

6.1.3 Vital Services

Digital identification and digital signing – the primary electronic functions of the Estonian ID-card – are listed as Vital Services in the Estonian Emergency Act. It becomes evident that human lives depend on the flawless functioning of the ID-card. It appeared that during the ROCA crisis, some of the Vital Services did not have an alternative authentication method available except from the eID. With this, the risk to the provision of vital services, and thus to human lives, was tangible. *"The fact that the ID-card became a vital service, was also correct, lives are dependent on it. If a doctor cannot access medical records, then someone might die because of it."*

The interviewees explained that the Estonian Emergency Act lacks clarity[1] on what is considered a Vital Service, and under which circumstances the Vital Service is

[1] The interviews are conducted in February-April 2018.

considered being interrupted. It was questioned if, for example, the software that the Vital Service is running on, should also be considered a part of that Vital Service under HOS (and therefore be under the State's closer supervision)? *"I think there is room for interpretation. HOS says that authentication and digital signing is a Vital Service, but it has not put down the limits. If we can authenticate and sign with 100 cards, but the other 1,2 million do not work, is then the Vital Service ensured?"*

Regulating Vital Services in the ICT sector presents challenges as the fast-evolving technology makes it hard to establish firmly fixed emergency and operational procedures in the State institutions. The Estonian e-ecosystem, and the variety of public services offered electronically by the State, constitutes a complex system with many variables. This further complicates setting up fixed procedures. *"Using info systems is still quite new, we've used it for 10-15 years. Not all procedures have developed yet, and the world evolves much faster than bureaucracy can follow up on."*

6.1.4 Alternative Authentication Methods

The respondents considered the need for an alternative authentication and signing tool in order to back up the ID-card as one of the biggest lessons learned from the crisis. Until the emergence of the ROCA vulnerability, the other alternative authentication tools, namely the mID and the Smart-ID, were seen as competing solutions to the ID-card. No one realised that having an alternative authentication tool is, in fact, a crucial security measure. *"There is a recommendation, that there should be a secondary authentication possibility that is seen as secure. With the m-ID we didn't see a big increase in usage during the crisis."*

The interviewees reported that the ROCA case clearly demonstrated that the existence of alternative authentication tools alone does not solve the related security risks. The end-users bear a responsibility for active uptake of the alternative authentication tools in a secure and responsible manner. *"When we have a focal service, like the e-ID, then we have to think through the alternatives, users have to duplicate their end also, e.g. the support for m-ID on services."*

Importantly, there is no alternative to the x-Road. It was suggested that rather than developing a duplicate, the State should be ready to develop an alternative means promptly when the need arises.

The ROCA case demonstrated that the existence and availability of alternative authentication methods as well as the supporting technological solutions are required for the safe and reliable provision of eID solutions by the State.

Mobile-ID

The mobile-ID presented a secure alternative to the ID-card during the ROCA case. However, due to the cumbersome procedure, the uptake of the mID was not particularly high compared to the number of ID-cards. *"One thing not affected by the security risks, was the m-ID. You can activate your m-ID using your ID-card."*

As the case unrolled, it became evident that despite the mID serves as an alternative means for authentication and digital signing, it failed to act as a back-up service for the majority of the population as its set-up process was tied to the ID-card. The telecom companies were not allowed to activate the mID service for new applicants unless they had a valid ID-card certificates. With invalid certificates, the user still needed to visit the PPA service point in person for authentication and mID service activation. It became clear that the use of the ID-card for the mID service activation constitutes yet another a single point of failure.

It was therefore proposed by the interviewees that the mID should be legally regulated as an independent process and its set-up procedure to become independent form the ID-card. Untying the mID form from the ID-card was approached as a means to mitigate the crisis, yet, finding such a long-term solution was not feasible in the given timeframe.

Importantly, once the user is authenticated and the mID service is activated, the mID is no longer dependent on the ID-card and can be used as an alternative means for digital authentication and signing. At the time of the ROCA crisis, the principle problem was that not enough people had the mID service already activated.

Smart-ID

The commercial banks in Estonia have initiated the launch of yet another digital authentication and signing tool: The Smart-ID. At the time of the ROCA crisis, the Estonian Smart-ID was undergoing a process of receiving the QSCD stamp to be listed as a qualified trust service for giving eIDAS qualified digital signatures. As of November 2018, the Smart-ID is recognised as a Qualified Signature Creation Device and enables giving Certified Digital Signatures similarly to the ID-card and mID.

6.2 Impact on the Information Society

This sub-topic discusses how the Estonian information society and democratic processes were affected by the ROCA case as well as the end-users' trust towards the eID and Estonia's image internationally.

6.2.1 Trust and Democracy

The interviewees reported that during early stages of the ROCA case, there was high uncertainty towards how big effect the security flaw would have on internet voting during the imminent local elections in Estonia in October 2017.

From domestic policy perspective, a political message by the Estonian Prime Minister, given soon after the ROCA vulnerability became public, had a strong influence on public perception of the ROCA case. Despite that the Prime Minister's party was widely known opponent of i-voting, the Prime Minister gave a clear message to the public that the fault in the ID-card chip is going to be fixed and that the State stands strongly behind the eID concept. This gave the public a strong message that the e-State, including internet voting, is and will remain credible. In addition, a number of risk assessments were compiled for the Electoral Committee to prepare for the elections.

The electoral outcomes proved that trust in the e-State remained high despite the ROCA case. The usage of the ID-card remained high throughout the ROCA case and the 2017 local elections presented the highest i-voter turnout in Estonian history[1].

It was mentioned by the interviewees that there is a general belief among the vast majority of population, including the people employed in the State sector, that nothing can go wrong in the realm of cyber security and information technologies. This results in low levels of compliance with the basic cyber security instructions, often referred to as cyber hygiene, which include making regular back-ups or recommended updates to the information systems. *"Most people don't believe that you could get damaged with cyber. They believe it will not happen to them. And then they trust. If we talk about cyber hygiene – even though it is always told: "Make back-ups", then the people make them only after there has been a serious accident."*

This general belief may have been diminished in some extent by the ROCA case as an incident has occurred and the security of the e-services cannot be taken for granted. In the eyes of an average citizen, the threat and the related media noise translated into knowledge that an element of the e-State failed. *"The sense, that IT is delicate, wasn't as clear before. The trust for the technology in general, not for the ID-card or for the State, decreased."*

On the other hand, it can be said that the trust and the way how the swift usage of the eID is enwoven into the daily life, was the key reason behind such a low level of awareness of the possible security risks and the end-user's overall dependence on the eID. An example from the medical system is following: *"No one believed it would be this bad. Many wanted a re-assurance that this is not an exercise, they didn't believe it, because it was such a bad situation."*

The Estonia population has grown highly accustom to the convenience the e-services offer. This strongly influences the users' attitudes towards security and facilitates trust. It is generally believed that if an IT solution works, it must be safe. At the occurrence of threats or failures, people expect the faults to be fixed without a delay. Returning to a non-digital alternative (handwritten signatures and visiting State offices in person) is not

[1] (https://kov2017.valimised.ee/valimistulemus-vald.html)

considered as an option. *"People in Estonia are so used to using these e-solutions, that they are not willing to go back on paper. They do not even want to think about it. If something is not working, fix it. Trust towards the State is high." "I think convenience outweighs trust issues. If we talk about reputation-loss, then I do not know how bad things should be for people to actually go back to paper systems. The big cases will (maybe) start decreasing the trust."*

In its public information campaign, the State managed to convey to the public a message that the ROCA vulnerability only posed a theoretical threat and no incident took place, using the eID remained safe throughout the ROCA case.

The interviews mention that the State encountered a similar crisis in 2011, however, at that time, the public and the end-user was not informed about the threat. It is inferred to several times that the decision to inform the user-base about the ROCA vulnerability had a positive effect on transparency and retaining the trust towards the Sate.

From an image perspective, the ROCA case posed a valid threat to Estonia's overall image as an e-State. The breakdown of only one ID-card would have been enough to discredit the foundation on which the Estonian e-State stands on. But not only: the i-voting pioneered in Estonia and the e-Residency project could have been fundamentally discredited at the event of an electronic vote-rigging or falsification of an e-Signature. *"A journalist doesn't care about that. If the FSB would buy just 1 vote, then we cannot say this did not happen, this is enough for a PR attack."*

The Estonian State was successful in keeping an image of secure electronic identity and internet voting during and after the ROCA case. Trust towards the eID remained high despite the security risk posed by the ROCA vulnerability. In the eyes of the end-user, the convenience of using the eID outweighs possible security concerns. In case of a fault or a threat, immediate fix is expected from the State.

6.2.2 Privacy and Transparency

Another topic that emerges from the interviews is the extent in which the State should have access to the ID-card user data. While the knowledge about the different user groups and detailed user activity would be useful for crisis management and crisis communication in the future, the interviewees feared that having access to user data could potentially mean bypassing user privacy. It was stated in several occasions that the State does not want, in principle, to have such a “backdoor access” as it would be seen as violation of privacy of individual eID users and cost the State a loss in credibility. *“The principle is, that the State guarantees, that there is no “backdoor access” to the ID-card usage, then there can’t be any access. It is a question of principle.”*

Instead, the State continues to rely on the user information provided by the certification centre SK. It was stated by the interviewees that if the State knows what to ask for, the time needed to complete the query to SK is reasonably short (1 day). *“But it has two ends: from the State view it would be useful to have this info to orientate quickly. In reality, the inquiry of user activity is an inquiry to private life, I get the info from the certification centre. An ordinary person does not like these kinds of inquiries, especially if it done by the Police.”* Alternative opinions suggested accessing the user data by using solutions which would solely rely on metrics and impersonalised user information.

6.2.3 Estonia’s Image Abroad

The relatively short time that was needed to overcome the ROCA vulnerability helped Estonia to maintain its strong image among international partners with awareness and interest in the information technology field. Estonia’s image as a strong e-society (e-State) provides a leverage on the international market. Big IT companies are interested in winning a contract with the Estonian State. *“The ones that know us as an e-State were positive about how fast the problem was solved. In other countries, solving a problem like this would not be possible as fast. This makes us special.”*

Besides the ID-cards for the Estonian citizens, the e-Residence cards and the diplomat ID-s were affected. The Ministry of Foreign Affairs was involved in the communication with Estonians living abroad and the e-Residents (via embassies). Only few e-Residents had difficulties with the renewal of certificates, other than that, the embassies faced no outward problems during the crisis resolution. The embassies themselves did not possess alternative authentication means and had to invent ways how to keep their everyday information systems running.

International media was monitored on this topic, yet the ROCA case in Estonia went internationally unnoticed at large. *"We should've used this narrative more strongly in the world: like in 2007, when other countries just closed down, we chose another way and fought. We had some coverage, but not a lot. We could have had image effects. It wasn't noticed in the world."*

6.3 Conclusions of the theme "End User"

This section provides an answer to the sub-research question: Which obligations and opportunities for the eID end-users emerge from the ROCA case?

The Estonian eID end-users can be divided into two categories: The State and individual eID users.

The interviews reveal that in Estonia, the State's guarantee on the safety of the digital ecosystem, and the extent in which the society relies on the digital ecosystem, is exceptional. The eID infrastructure is fundamental enabler for the basic functioning of both, the private and the State sector.

Furthermore, the State is recognised as the primary end-user of the eID. The daily functioning of its institutions and the provision of public services is built on the use of the eID and the x-Road. The underlying importance of the eID for the Estonian State is that there are some State services that only exist in the electronic version, i.e. are fully dependent on the digital ecosystem and its key enabling elements, the eID and the x-Road.

The ROCA vulnerability strongly impacted the Estonian e-ecosystem and its individual members, that is to say, the whole Estonian information society. As mentioned earlier in the analysis, the concept of identity has changed via the use of the eID. The eID is not only a means for identification but is an enabler for broader participation in democratic processes, two-way communication between the State and the citizen; enabler and simplifier for business activity. By enabling internet voting, the eID is enhancing broader participation in elections in Estonia and thus directly influencing the country's democratic processes.

In Theme 3: "End User", the State as an actor is analysed from the eID end user perspective whereas in the Theme 1: "State and Policies" the State is analysed from the policy maker perspective. However, it is visible that despite these different perspectives, the State's responsibilities overlap. It is natural as the State as an actor is in fact a part of the larger unit, the country's e-ecosystem. The State is the provider of key elements of the country's digital infrastructure (such as the eID and the x-Road) and has regulatory power over the digital ecosystem. Therefore, the State as an actor has strong impact on the country's digital ecosystem. Nevertheless, it becomes evident form the interviews that both, the State, and the country's whole digital ecosystem (individual and commercial end users together) are highly dependent on the Estonian eID.

Obligations arising for the State from the use of eID:

- *The State's primary responsibility is to maintain of the key elements of the e-ecosystem*, including the flawless functioning of the eID and the x-Road. It emerges from the ROCA case that there is a variety of elements and tasks within the e-ecosystem that require oversight with a high level of technical expertise. Yet, it is necessary to reach an agreement on the extent of the State's responsibility to maintain the different elements of the e-ecosystem.

- *The State has a responsibility to maintain the Vital Services, the eID among them*. It becomes evident that human lives depend on the flawless functioning of the eID. It appeared that during the ROCA crisis, some of the Vital Services did not have an alternative authentication method available except from the eID.

- *The State's responsibility is to know thoroughly the elements of the State administration which are dependent on the eID.* This requires mapping all public services dependent on the eID. The ROCA case revealed that the State was unaware of the depth and extent of its dependence on the eID in 2017.

- *It is necessary to reach to an agreement what constitutes a "dependency" on the eID.* It became evident during the ROCA case that adding a definition or a desirable level of service quality to the existing operational guidelines or legal framework is necessary.

- *Bringing all the State institutions to comparable levels of technological preparedness* would enable swift crisis response from the State. This was demonstrated by the difficulties that arose during and after the remote renewal of the ID-card certificates during the ROCA case.

- *Ensuring security of the eID service while making sure the privacy of the end-users is not compromised.* The ROCA case showed that the knowledge of the eID user behaviour was missing. This curbed the State's ability to segment the ID-card users into user groups based on their differing needs for information and technical assistance. Segmented communication may prove useful for targeted crisis communication and response in the future.

- *Determining which (State) institutions are responsible for which elements of the eID area.* The ROCA case revealed that the responsibility over the eID area is fragmented between different institutions and private sector entities. It was realised amidst the ROCA case that the lines of responsibility were not always clearly determined. None of these actors alone had full oversight nor control over the eID area in Estonia during the ROCA case.

- *Enabling and coordinating effective cooperation between the different institutions and stakeholders of the digital ecosystem.* The ROCA vulnerability and the resulting crisis revealed insufficient coordination among all related parties. At the time of the ROCA crisis, there was no single cooperating and controlling body over the Estonian e-ecosystem.

- *The State's responsibility is to create a fitting legal framework for providing alternative electronic authentication tools and supportive services.* The availability of multiple authentication mechanisms minimises security risks. This would also avoid allowing single points of failure such as presented by SK in the role of certification provider or the x-Road as the single interoperability platform for the entire e-ecosystem. The ROCA case demonstrated that the existence and availability of alternative authentication methods as well as the supporting technological solutions are required for the safe and reliable provision of eID solutions by the State.

The opportunities that emerge from the use of the eID for the State:

- *The State to benefits from high levels of trust by its residents,* shown by the wide usage of the State-provided eID. The positive culmination of the ROCA case allows the State to continue pursuing its digital agenda overall. The 2017 i-voting outcomes in Estonia proved that trust in the eID and the e-State remained high despite the ROCA case.

- *The eID emerges as a tool to enhance democratic participation* by enabling internet voting. The use of the eID broadens access to voting and therefore influences democratic processes in Estonia. The 2017 local elections in Estonia saw the highest i-voting turnout in Estonian history.

- *The eID serves Estonia for positive image building* and the dedication to further developing the e-State allows Estonia to “punch above its weight” in creating pioneering technologies and concepts such as the e-Residency, data embassies etc. The ROCA case caused the Estonian State minimal amount of negative attention in international media but allowed the country to prove itself as a trustworthy and capable e-society considering the speed in which the ROCA case was solved.

The individual end-user’s obligations emerging from the ROCA case:

- *Recognising its dependence on the eID and taking active approach towards the eID usage*. The interviews suggest that the citizen takes the State’s guarantee for the security of the eID for granted. This is reflected in the general attitudes which were prevalent in Estonia during the ROCA case. According to these, nothing can happen to the State-provided ICT solutions and if an incident indeed occurs, an immediate fix is expected. The citizen is not considering returning to a non-digital alternative of an e-service.

- *Following the State's instructions regarding updating their devices* (or ID-card certificates in that particular case) and general recommendations on cyber-hygiene and security. The ROCA case demonstrated that active involvement from the end-user's part is necessary for the up keeping of the eID service.

- *Opting in for the alternative electronic authentication means available.* One of the biggest lessons learned from the ROCA case was the need for an alternative authentication and signing tool to back up the ID-card. The end-users bear a responsibility for active uptake of the alternative authentication tools in a secure and responsible manner.

Opportunities for the individual end-user:

- *Reliance on the eID in business models and communication channels*. The Estonian State's strong political confirmation to the continuation of the e-State and the uninterrupted availability of the eID despite the ROCA case sent a strong signal to the public that faults get fixed rather than services taken down. This showed the individual end-user that the State continues to support and propagate the eID and with this guarantee, further economic opportunities arise for the citizen.

- *Opportunity to participate in democratic processes.* The eID was available to the end-users throughout the ROCA case and was used for internet-voting during the 2017 local municipality elections. The i-voting turnout was the highest in Estonian history.

- *Opportunity to contribute to the development and up keeping* of the eID area. A need for creating a wider ICT community which would involve experts with different backgrounds arose from the analysis of the ROCA case. This network of experts would contribute to information sharing as well as to the up scaling of the State's capacities to address challenges arising in the eID field.

7 Conclusions and discussion

This chapter provides an answer to the main research question of this thesis: What implications does the ROCA case present on State-provided eID? The research findings are then placed into context with the relevant academic literature to provide the reader with a fuller overview.

The thematic analysis uncovers a detailed view of the aspects surrounding the provision of electronic identification by the Estonian State. The 2017 ROCA case in Estonia uncovers many aspects about the Estonian e-ecosystem and the eID. Moreover, the ROCA case revelas that there are new, unprecedented responsibilities and roles for the State to fulfill regarding the provision of the national eID.

7.1 eID Management

Following the ROCA case, the eID management in Estonia emerges on a new level of maturation. The eID is well taken into use and the society along with the State administration is relying on the eID in its daily operations in an increasing rate. The eID constitutes a basic infrastructre which enables both, the State administration along with its public services, and the private sector, to carry out various transactions and communication. Based on the ROCA case, it is fair to say that the Estonian State encounters vast and unprecedented dependency on its eID. The Estonian State is recognised as the primary end-user of the eID. Much until the 2017 ROCA case, the eID management in Estona appears to have been an optional, experimental, and as-needed based sphere (Kattel and Mergel, 2019). In consequence of the ROCA case, *the eID management area is now recognised as an area that needs to be thoroughly planned, developed and secured.*

Simialr conclusions are reached in other studies and analyses conducted about the 2017 ROCA case in Estonia. A study commissioned by the RIA and conducted by the Tallinn

University of Technology, points out a series of anticipated improvements in the Estonian eID area, mainly in the political oversight and crisis management functions by the Estonian State (Buldas *et al.*, 2018)). Moreover, Lips et al. (2019) list the positive effects of the ROCA case on the overall eID management in Estonia: improved crisis management readiness, heightened awareness of the eID and the eID security as well as underlined the importance of public-private sector cooperation.

The ROCA case serves as a ground for continuity planning and risk management for public and private entities alike (Information System Authority, 2018a). Moreover, two comprehensive strategy documents – the White Book on Identity Management and Identity Documetnts 1.0 (E-Estonia Council, 2018) and the Digital Agenda 2020 for Estonia (Ministry of Economic Affairs and Communications, 2018) have been compiled taking into account the lessons learned from the ROCA case. These documents provide the basis for ensuring the security and reliability of both the eID technology and the digital identity document issuing process (Invest In Estonia, 2019) as well as for the development of a mature and secure environment for the widespread use of smart ICT solutions (Ministry of Economic Affairs and Communications, 2019).

The TalTech study along with this thesis points out the need for acknowledging the importance of the eID for the Estonian digital ecosystem and taking full political responsibility deriving from that. Through its dependency on the eID and the long-term political guarantee it has given to its citizens and residents, the State is obliged to guarantee the continuity of the digital identity document and all the related infrastructure elements. Therefore, *the primary responsibility for the State in the eID area is to upkeep and guarantee the security of the eID service. Likewise, upkeeping the respective infrastructure and related parts of the nation's digital ecosystem has thus also become an undeniable obligation for the Estonian State.*

Considering the large number ID-cards affected by the ROCA vulnerability and the end-users' high dependence on the Estonian eID, the ROCA case was considered a highly sensitive and large-scale security issue for the Estonian State (Lips *et al.*, 2018). The success in handling that security threat by the Estonian authorities is viewed as a result of effective and agile management, which relied heavily on public-private partnerships, openness (transparent public communication), technological advances of the country, and continuous reviews and analysis of its performance (Ibid.).

The eID is not only a key enabler within the Estonian e-ecosystem. The ROCA case in Estonia showed that the Estonian population trusts and is reliant on the eID in a wide extent. With the clearly expressed political direction by the State and the State’s extensive guarantee for the reliability of the eID, there has grown a justified expectation from the population towards the State that the eID is available to all end-users and that the service is uninterrupted, secure and widely functional. The end-user reactions to the ROCA case allow to suggest that *the eID is percieved as a right* for the Estonian citizens and residents.

In Estonia, having an electronic identity document is established as the norm. In Estonia, the electronic identity is the digital representation of the person’s physical identity. The person’s digital identity is only one, even when it may be carried by more than one digital tokens (Riigikogu, 1999; Information System Authority, 2019).

The Estonian eID therefore represents an extention of the concept of a physical identity document into the digital realm. The State’s responsibility to provide the eID – a digital identity document - equals with the responsibility of providing all other identity documents. The development of this phenomen should be seen as an analogy to the extension of legal regulations or the State’s administrative procedures into the digital realm. The principle remains the same: what is accessible in the physical realm, needs to be likewise accessible in a digital environment. Some thinkers such as Linnar Viik take this notion even broader by calling the eID „*an extension of public infrastructure; the 21st-century version of the welfare state.“* (Keen, 2018).

The dynamics between the State and the resident now applies also in reversed fashion: what the State made obligatory for the citizen in the rollout phase of the ID-cards and eID’s in early 2000’s (Palginõmm, 2016), has now become an obligation for the State to deliver and upkeep for its citizens and residents. Thus, the ROCA case demonstrates that *providing the eID is not anymore a voluntary option for the Estonian State, it has become an obligation.*

It was concluded in the research material that the concept of identity has changed in Estonia due to widespread use of the eID. Not only is it an identity document, but together with the Estonian x-Road it has become an enabler, a connector of business and public spheres; the citizen and the State in reciprocal manner. The eID bears equal legal value as the national passport and the digital signatures given via the use of the eID equal with handwritten signatures.

The above listed elaborated patterns in user behaviour within the Estonian e-ecosystem allow to consider socio-technical effects of the State-provided eID. The eID is not only a means for identification but is an enabler for broader participation in democratic processes, two-way communication between the State and the citizen; enabler and simplifier for business activity. The 2017 ROCA case in Estonia demonstrates that the way and the extent in which the Estonian society has rearranged itself as a result of *the widespread use of the eID, gives proof of a significant socio-technical effect.*

7.2 The State, Market, and International Regulation

The thematic analysis revealed that *the State is in a versatile role as a provider of electronic identity*. This puts the State on a borderline where public and private spheres meet; where national sovereignty and international regulation become intertwined. The State's interactions with other actors on the ICT market and finding the balance between domestic and inter-state legal regulation become increasingly important.

The ROCA case reveals *challenges in the interaction between the State and the EU in terms of regulation and procedure.* While considering conventional identity documents such as national passports and ID-cards, the responsibility to ensure the security and authenticity of these documents lies entirely on the State issuing these documents. In the digital realm, the European Union has the oversight as stipulated by the eIDAS regulation (European Parliament, 2014). The ROCA case revealed two weaknesses of the current European setting for electronic identity management: the European Union crisis notification mechanism was seen as largely insufficient; as a consequence, the whole Estonian e-ecosystem, through its dependence on the eID, was put in risk. Thus, the Estonian Information System Authority makes a potent claim for the EU MS's to compare the interpretation and the emerging practice of Article 19 of the eIDAS regulation (Information System Authority, 2018a).

Second, it was stated in the thematic analysis that the European cybersecurity certification framework does little to truly provide security and trust among the EU Member States and was seen as a market barrier by the interviewees. The purpose of the EU cybersecurity certification framework under the Cyber Security Act is to establish and maintain the trust and security on cybersecurity products, services, and processes. This is to allow the end-users and service providers to determine the level of security assurance of the products, services and processes they procure, make available or use (ENISA, 2020b). However, it is yet to be seen if the latest updates concerning this framework currently being drafted by ENISA (ENISA, 2020a) provide an answer to this criticism.

Alongside with the use of digital identity**,** *the State has another new responsibility: to be capable of verifying identity (provided by a public or commercial entity) in a digital environment.* This responsibility is less talked about, yet crucial aspect considering the global trends in identity management. Accepting other forms of digital identities is made easy within the EU where exists a unified legal regulation for the provision of electronic identity – eIDAS – which includes a reciprocity clause: all certified Trust Services put forward by one EU Member State must be accepted by the rest of the EU Member States (European Commission, 2018). This offers a fairly large level playing field for the EU MS to develop their own electronic identities and is a big step towards truly enabling the European Digital Single Market.

However, this is not the case with other types of electronic identities available (i.e. those national or commercial solutions which do not comply with the specifications envisaged for the European Trust Services in the eIDAS regulation). Moreover, there is not even a clarity in the definition of what an electronic identity is. Many authors see it as a broad concept like Hoikkanen (2010): the sum or set of data that is electronically available and connected to one specific individual, including authentication details such as name, date of birth, gender, nationality as well as different information about that persons consumer behaviour, social profiles, business credentials and more. The eIDAS puts forward a narrower definition: the “electronic identity” is created and used in the purpose of authenticating a person in online business, commercial or administrative transactions

(European Parliament, 2014). The Estonian Identity Documents Act however defines electronic identity (eID) as an electronic identity document.

This broad spectrum of ideas regarding what an electronic identity is sets the scene where the Estonian eID along with the other European Union Trust Services meet with other versions of electronic identities. The American and Chinese approaches as described by van Dijck (2020) both provide a wide basis for discussion, future research, and visioning. Importantly, the Estonian Identity Management and Identity Documents White Book (2018), a 10-year development plan, foresees international cooperation with international electronic identification providers, as well as expresses the readiness to act as a go-between for the Estonian e-service providers for accepting eID's of non-EU countries (such as GSMA MobileConnect or Chinese CITIC, among others). Furthermore, the same document proposes to analyse whether, and in which extent, would Estonia be ready to allow the use of the Estonian eID with large international service providers Facebook, eBay, Google etc..

The State as an electronic identity provider is in a challenging position on the international ICT market. *There appears to be a clear clash between the private sector business interests and the State's responsibility to guarantee service quality, security, and uninterrupted availability*. As displayed by the ROCA case, public-private partnerships are inevitable in the Estonian eID supply chain. While the State wins form purchasing its software solutions and other products from the private sector providers, there is a trade-off as the State is influenced by the business interests of those private sector companies and has to give up a certain amount of control and confidentiality by consuming the private sector services and products. As revealed in the thematic analysis, some experts find it desirable to acquire more control over the eID supply chain by developing certain capabilities within the State infrastructure. The White Book on Identity Management and Identity Documents discloses the need to analyse the practicality of developing the capacity of providing qualified Trust Services by the Estonian State for the purpose of national security (E-Estonia Council, 2018). This comes in the backdrop of tighter concentration of competences and technologies on the international market for identity carriers, as well as clearer division of market share between the larger service providers (Ibid.).

In contrast with the international market and as an interesting phenomenon, the public-private cooperation within Estonian domestic e-ecosystem is portrayed as constructive and helpful in the research material. As the 2017 ROCA case emerged, a number of public and private sector stakeholders together with individual ICT experts voluntarily offered the State their help; without mentioning contracts, payments, or other business interests. As concluded by Lips *et al.*, (2018), it was clear after this experience that in complex situations the cooperation between public and private sector in Estonia is very advantageous.

The ROCA case demonstrated that the people engaged in crisis management process carried common values towards their work and the State, irrespective if they represented a private or public sector stakeholder. The attitude and prevalent work ethics within the organisations played equally important role as the institutional hierarchy and formally established workflows. This aspect was described as the "the Estonian cooperation model" in the interviews. Hence, *the "Estonian cooperation model" played an important role in the successful solving of the ROCA case in Estonia*.

Kattel and Mergel (2019) give an extensive explanation to this phenomenon in their recent article. In their perspective, in Estonia exists an informal, agile, and extremely close-knit network of high-profile politicians and their private sector IT advisers that continually seek mutual advice and guidance. This network has emerged as a historic evolvement of the Estonian ICT sector starting from early nineties, along with the rebuilding efforts of the Estonian State administration. According to Kattel and Mergel, reliance on this public-private network is one of the fundamental governance principles upon which the whole Estonian digital transformation is built.

Furthermore, the “Estonian Cooperation Model” can be viewed through the Koppenjan and Groenewegen’s model for institutional design; more precisely through the different layers of institutions and their (inter)action. The first layer “Actors and Games” concerning the *“actors/agents and their interactions aimed at creating and influencing (infrastructural) provisions, services, outcomes”* (Koppenjan and Groenewegen, 2005) represents the independent interests of those actors present in the Estonian ICT sector network. The second layer “Formal and informal institutional arrangements” which represents *“gentleman agreements, covenants, contracts, alliances, joint-ventures, merges, etc.”* (Ibid.) displays how the policies driving Estonia’s digital transformation evolved hand-in-hand with the pursuit of business interests of the banking and telecom companies in Estonia. (Kattel and Mergel, 2019). Following, the third layer “Formal institutional environment” which depicts the *“formal rules, laws and regulations, constitutions (formal institutions)”*(Koppenjan and Groenewegen, 2005) shows how these early developments of the Estonian State ICT area likely gave a reason and direction for developing the respective legislation in Estonia. The fourth and final layer “Informal institutional environment of socio-technical systems”, contains *“norms, values, orientation, codes (in-formal institutions, culture)”* (Ibid.). The work attitudes and unanimous approach towards resolving the ROCA case as described above as the “Estonian cooperation model” show how these contracts and underlying principles set up in the first and second layer are translated into the organisational culture and informal contact making in the fourth layer; and partially even allowed to bypass the normative framework presented in the third layer. This indicates that the State ICT sector is very strongly driven by those foundational principles which evolved together with the modern Estonian State since the 1990’s; and which now translate into actions on the surface level and are visible in individual actor’s behaviour, as displayed by the 2017 ROCA case.

The ”Estonian Cooperation Model” is perhaps most fittingly explained by Koppenjan and Groenewegen as follows: *“It is difficult to change institutions consciously since, to a large extent, they have been created along informal and incremental processes: they are the manifestation of unique, historical learning experiences of parties that have interacted over a longer period of time in a specific context and have developed rules on that basis.”(Ibid.)*

7.3 Limitations

This thesis presents a narrative and attempts to underline the socio-technical effect caused by the wide-spread use of eID in Estonia. Yet, the research material is indeed very deep (as presented in the chapters 4, 5, and 6 of this thesis) and is inviting for further analysis based on different theoretical perspectives.

7.4 Areas for further research

A thorough analysis of the Estonian eID management process based on Koppenjan and Groenewegen’s model of institutional design may prove enriching. The State’s interplay, cooperation, and conflicts of interests with private sector entities, expanding beyond Estonia’s domestic market, provides an interesting scene to analyse and contextualise. It would be interesting to find out if the model allows to gain a deeper understanding of the Estonian eID area’s institutional design and perhaps suggests improvements to the current set-up?

A necessity remains to better define the term electronic identity (eID) in academic literature and offer wider selection of terminology to depict the many differing versions of collections of personal data available digitally.

8 Summary

The purpose of this thesis is to provide a detailed overview of the 2017 ROCA case in Estonia and to understand what implications does such large-scale security risk pose on state-provided electronic identification mechanism.

The research is based on 32 semi-structured intervirews conducted with 41 Estonian high-level experts that were closely involved in solving of the ROCA case. These interviews provide a deep insight of the crisis management process as well as into the Estonian eID area. The research was concluded by using thematic analyse approach and with the use of NVIVO qualitative data analysis software.

The research results indicate that the primary responsibility for the State in the eID area is to upkeep and guarantee the security of the eID service. To this end, upkeeping the respective infrastructure and related parts of the nation's digital ecosystem has also become an undeniable obligation for the Estonian State.

The sociotechnical effect that using the eID has on the Estonian society is illustrated by the fact that the eID is percieved as a right by the Estonian citizens and residents. Thus, the provision of the electronic identity is no longer a voluntary option for the Estonian State, but has become an undeniable obligation.

In the context of European market for ICT products and services, the State is in a versatile role as a provider of electronic identity. Challenges arose in the interaction between Estonia and the EU in terms of regulation and procedure. In view of global identity management trends, the State is challenged by a new responsibility – to be capable of verifying third-party digital identities.

Another important implication for eID security is maintaining State control over the elements of the eID supply chain. In a market situation, the State is faced with a continuous dilemma whether to rely on external service providers or become the developer itself. While there appears to be a clear clash between the private sector

business interests and the State’s responsibility to guarantee service quality, security, and uninterrupted availability, a model of domestic public-private partnerships, intrinsic to Estonia, has played an important role in the successful solving of the ROCA case in Estonia.

The author’s proposals for further discussion on eID management includes rethinking the definition of eID in the light of the Estonian example and acknowledging the paradigm shift that already has taken place in Estonia for recognising the electronic identity as the citizens‘ right and its provision the State’s obligation.

References

[1] Bharosa, N., Lips, S. and Draheim, D. (2020), “Making e-Government Work Learning from the Netherlands and Estonia”, *EGOV-CeDEM-ePart 2020 Sweden, 31.08-02.09.2020.*, No. Forthcoming.

[2] Braun, V. and Clarke, V. (2006), “Using thematic analysis in psychology”, *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77–101.

[3] Buldas, A., Jung, M., Kuivjõgi, K., Tallinn, L., Osula, A.-M., Ottis, R., Priisalu, J. and Vaks, T. (2018), *ID-Kaardi kaasuse õppetunnid*, Tallinn.

[4] Drechsler, W. (2018), “Pathfinder: e-Estonia as the β-version”, *JeDEM - eJournal of eDemocracy and Open Government*, Vol. 10 No. 2, pp. 1–22.

[5] E-Estonia Council (2018), *Valge raamat: Identiteedihaldus ja isikut tõendavad dokumendid 1.0*, available at: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/eesti_infouhiskonna_arengukava_2020_0.pdf (accessed 23 July 2020).

[6] ENISA (2020a), “Cybersecurity Certification: EUCC Candidate Scheme”, available at: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/ (accessed 25 July 2020).

[7] ENISA (2020b), “EU cybersecurity certification framework”, available at: https://www.enisa.europa.eu/topics/standards/certification (accessed 25 July 2020).

[8] Enterprise Estonia (2019), “KSI Blockchain”, available at: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain (accessed 27 July 2020).

[9] Enterprise Estonia (2020a), “e-Estonia Facts”, available at: https://e-estonia.com/wp-content/uploads/e-estonia-facts-19-08-23.pdf (accessed 27 July 2020).

[10] Enterprise Estonia (2020b), “e-Identity”, available at: https://e-estonia.com/solutions/e-identity/id-card (accessed 27 July 2020).

[11] European Commission (2018), “Digital Single Market. e-Identification”, Policy, available at: https://ec.europa.eu/digital-single-market/en/e-identification (accessed 5 January 2019).

[12] European Parliament (2014), *Regulation (EU) No 910/2014: eIDAS.*

[13] Ghaffarian, V. (2011), “The new stream of socio-technical approach and main stream information systems research”, *Procedia Computer Science*, Vol. 3, pp. 1499–1511.

[14] Hedström, K., Wihlborg, E., Gustafsson, M.S. and Söderström, F. (2015), “Constructing identities – professional use of eID in public organisations”, *Transforming Government: People, Process and Policy*, Vol. 9 No. 2, pp. 143–158.

[15] Hoikkanen, A., Bacigalupo, M., Lusoli, W., Maghiros, I. and Nikolov, S. (2010), “Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies”, in Leeuw, E. de, Fischer-Hübner, S. and Lothar, F. (Eds.), *Policies and research in identity management: Second IFIP WG 11.6 Working Conference, IDMAN 2010, Oslo, Norway, November 18-19, 2010, proceedings, IFIP AICT, 1571-5736*, Vol. 343, Springer-Verlag, Berlin, pp. 41–58.

[16] Information System Authority (2018a), “Estonia Offers Recommendations in the Light of eID Vulnerability”, available at: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html (accessed 25 July 2020).

[17] Information System Authority (2018b), *ROCA Vulnerability and eID: Lessons Learned*, available at: https://www.ria.ee/en/news/estonia-offers-recommendations-light-eid-vulnerability.html (accessed 19 July 2020).

[18] Information System Authority (2019), “Electronic Identity eID”, available at: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html (accessed 27 July 2020).

[19] Invest In Estonia (2019), “The e-Estonia Council supported the 10-year development plan for the ID-card and e-identity”, available at: https://investinestonia.com/the-e-estonia-council-supported-the-10-year-development-plan-for-the-id-card-and-e-identity/ (accessed 23 July 2020).

[20] Kattel, R. and Mergel, I. (2019), “Estonia’s Digital Transformation”, in Hart, P.'t. and Compton, M.E. (Eds.), *Great policy successes, or, A tale about why it's amazing that governments get so little credit for their many everday and extraordinary achievements as told by sympathetic observers who seek to create space for a less relentlessly negative view of our pivotal public institutions*, First edition, Oxford University Press, Oxford United Kingdom, New York NY, pp. 143–160.

[21] Keen, A. (2018), “Where in the world will you find the most advanced e-government? Estonia.”, available at: https://ideas.ted.com/where-in-the-world-will-you-find-the-most-advanced-e-government-estonia/ (accessed 22 July 2020).

[22] Koppenjan, J. and Groenewegen, J. (2005), “Institutional design for complex technological systems”, *International Journal of Technology, Policy and Management*, Vol. 5 No. 3, pp. 240–257.

[23] Latour, B. (1990), “Technology is Society Made Durable”, *The Sociological Review*, Vol. 38 No. 1_suppl, pp. 103–131.

[24] Lips, S., Pappel, I., Tsap, V. and Draheim, D. (2018), “Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field”, in Kő, A. and Francesconi, E. (Eds.), *Electronic government and the information systems perspective: 7th International Conference, EGOVIS 2018, Regensburg, Germany, September 3-5, 2018, Proceedings / edited by Andrea Kő, Enrico Francesconi, Lecture Notes in Computer Science, 0302-9743*, Vol. 11032, Springer, Cham, pp. 60–70.

[25] Margetts, H. and Naumann, A. (2016), *Government as a Platform: What Can Estonia Show the World*, Oxford, available at: https://www.politics.ox.ac.uk/materials/publications/16061/government-as-a-platform.pdf (accessed 27 July 2020).

[26] Ministry of Economic Affairs and Communications (2018), *Eesti Infoühiskonna Arengukava 2020*.

[27] Ministry of Economic Affairs and Communications (2019), “Information society. Digital Agenda 2020 for Estonia”, available at: https://mkm.ee/en/objectives-activities/information-society (accessed 23 July 2020).

[28] Nemec, M., Sys, M., Svenda, P., Klinec, D. and Matyas, V., “The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli”, pp. 1631–1648.

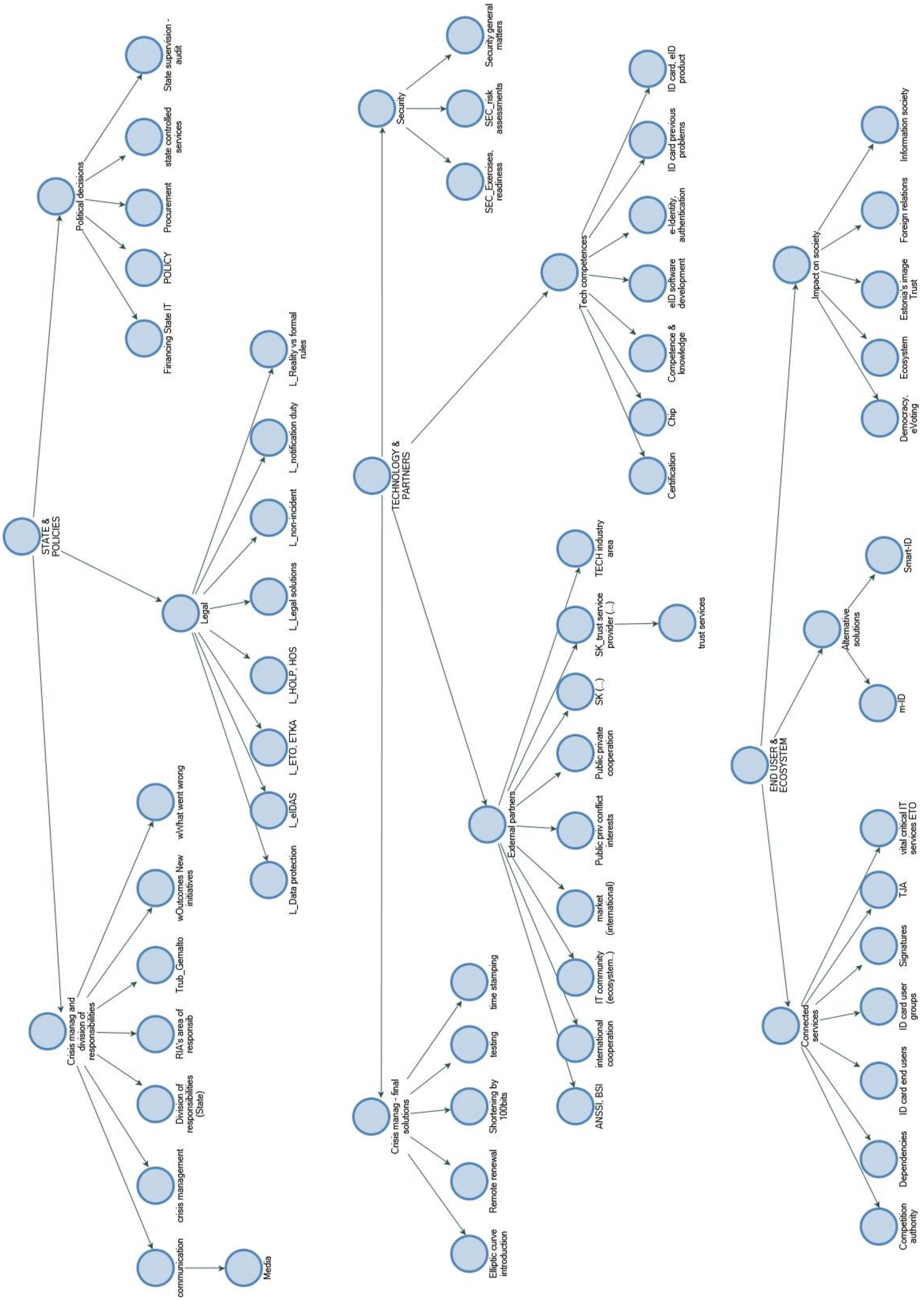
[29] Palginõmm, M.-L. (2016), “Diffusion of the Estonian ID-card and Its Electronic Usage: Explaining the Success Story”, Master's Thesis, Ragnar Nurkse School of Innovation and Governance, Tallinn University of technology, Tallinn, 2016.

[30] Riigikogu (1999), *Identity Documents Act: ITDS*.

[31] van Dijck, J. and Jacobs, B. (2020), “Electronic identity services as sociotechnical and political-economic constructs”, *New Media & Society*, Vol. 22 No. 5, pp. 896–914.

[32] Welsh, E. (2002), “Dealing with Data: Using NVivo in the Qualitative Data Analysis Process”, *Forum: Qualitative Social Research*, Vol. 3 No. 2.

Appendix 1 – Initial coding, thematic analysis phase 3.


STATE & POLICIES
Political decisions
State supervision - audit
state controlled services
Procurement
POLICY
Financing State IT
Legal
L_Reality vs formal rules
L_notification duty
L_non-incident
L_Legal solutions
L_HOLP, HOS
L_ETO, ETKA
L_eIDAS
L_Data protection
Crisis manag and division of responsibilities
wWhat went wrong
wOutcomes New initiatives
Trub_Gemalto
RIA's area of responsib
Division of responsibilities (State)
crisis management
communication
Media
TECHNOLOGY & PARTNERS
Security
Security general matters
SEC_risk assessments
SEC_Exercises, readiness
Tech competences
ID card, eID product
ID card previous problems
e-Identity, authentication
eID software development
Competence & knowledge
Chip
Certification
External partners
TECH industry area
SK_trust service provider (...)
trust services
SK (...)
Public private cooperation
Public priv conflict interests
market (international)
IT community (ecosystem..)
international cooperation
ANSSI, BSI
Crisis manag - final solutions
time stamping
testing
Shortening by 100bits
Remote renewal
Elliptic curve introduction
END USER & ECOSYSTEM
Impact on society
Information society
Foreign relations
Estonia's image Trust
Ecosystem
Democracy, eVoting
Alternative solutions
Smart-ID
m-ID
Connected services
vital critical IT services ETO
TJA
Signatures
ID card user groups
ID card end users
Dependencies
Competition authority