DOCTORAL THESIS

eID Public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity

Valentyna Tsap

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2022

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
12/2022

eID Public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity

VALENTYNA TSAP

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science

The dissertation was accepted for the defence of the degree of Doctor of Philosophy (Computer Science) on 19th of April 2022

Supervisor: Prof. Dr. Dirk Draheim
Information Systems Group
Department of Software Science
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Co-supervisor: Assoc.-Prof. Dr. Ingrid Pappel
Department of Software Science
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Opponents: Prof. Dr. Dr. Robert Krimmer
Johan Skytte Institute of Political Studies
University of Tartu
Tartu, Estonia

Prof. Dr. Nitesh Bharosa
Faculty of Technology, Policy and Management
Delft University of Technology
Delft, the Netherlands

Defence of the thesis: 18th of May 2022, Tallinn

Declaration:
Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology, has not been submitted for any academic degree elsewhere.

Valentyna Tsap

signature

ISSN 2585-6898 (publication)
ISBN 978-9949-83-811-0 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9949-83-812-7 (PDF)
Printed by Koopia Niini & Rauam

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
12/2022

eID avalik aktsepteerimine: edutegurid, kodanike pertseptsioon ja elektroonilise identiteedi mõju

VALENTYNA TSAP

TALTECH
KIRJASTUS

To my parents

Contents

List of Publications

The present Ph.D. thesis is based on the following publications that are referred to in the text by Roman numbers.

I V. Tsap, I. Pappel, and D. Draheim. Key success factors in introducing national e-identification systems. In T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, editors, *Proceedings of FDSE'2017 – 4th International Conference on the Future Data and Security Engineering*, volume 10646 of *Lecture Notes in Computer Science*, pages 455–471, Cham, 2017. Springer

II V. Tsap. e-Identity and eIDAS: Interpretation of concepts by different countries. In A.-M. Osula and O. Maennel, editors, *Proceedings of ICR'2018 – the 4th Interdisciplinary Cyber Research Workshop 2018*, pages 9–10. Tallinn University of Technology, Department of Software Science, 2018. [last accessed 5 Nov 2021]
https://haldus.taltech.ee/sites/default/files/2021-04/ICR2018_proceedings.pdf

III V. Tsap, I. Pappel, and D. Draheim. Factors affecting e-ID public acceptance: A literature review. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2019 – the 8th International Conference on Electronic Government and the Information Systems Perspective*, pages 176–188, Cham, 2019. Springer

IV V. Tsap, S. Lips, and D. Draheim. eID public acceptance in Estonia: towards understanding the citizen. In S.-J. Eom and J. Lee, editors, *Proceedings of dg.o'20 – the 21st Annual International Conference on Digital Government Research: Intelligent Government in the Intelligent Information Society*, pages 340–341. Association for Computing Machinery, 2020

V V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2020 – the 9th International Conference on Electronic Government and the Information Systems Perspective*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer

VI S. Lips, V. Tsap, I. Pappel, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In A. Kõ and E. Francesconi, editors, *Proceedings of EGOVIS'2018 - the 7th International Conference on Electronic Government and the Information Systems Perspective*, volume 11032 of *Lecture Notes in Computer Science*, pages 60–70, Cham, 2018. Springer

VII M. Tsulukidze, K. Nyman-Metcalf, V. Tsap, I. Pappel, and D. Draheim. Aspects of personal data protection from state and citizen perspectives – case of Georgia. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, and M. Mäntymäki, editors, *Proceedings of I3E'2019 – the 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society: Digital Transformation for a Sustainable Society in the 21st Century*, volume 11701 *of Lecture Notes in Computer Science*, pages 476–488, Cham, 2019. Springer

VIII A. Valtna-Dvořák, S. Lips, V. Tsap, R. Ottis, J. Priisalu, and D. Draheim. Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2021 – the 10th International Conference Electronic Government and the Information Systems Perspective*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer

IX A. R. Maerøe, A. Norta, V. Tsap, and I. Pappel. Increasing citizen participation in e-participatory budgeting processes. *Journal of Information Technology & Politics*, 18(2):125–147, 2021

Author's Contributions to the Publications

I First author. This paper was initially submitted as author's master's thesis. The author specified the research problem and objectives, conducted another round of data analysis, and wrote the manuscript under guidance of other co-authors. The author presented the publication at the Future Data and Security Engineering Conference in Ho Chi Ming City, Vietnam, 2017.

II First author. The author conducted literature review, identified the research problem, and described the linkage between the status quo of eIDAS interpretations among European states and the existing research works. The author wrote the text of the abstract.

III First author. The author identified the research topic and problem, selected suitable research methodology, conducted the systematic literature review, and wrote the manuscript. The author presented the publication at the International Conference on Electronic Government and the Information Systems Perspective in 2021.

IV First author. The author highlighted the research problem, conducted literature review, designed the questionnaire together with other co-authors, and wrote the manuscript. The author presented the publication online at International Conference on Digital Government Research in 2020.

V First author. The author specified the research problem described in [IV], distributed the questionnaire together with co-authors. The author solely analyzed the collected data consolidated from each questionnaire (Estonian, English, and Russian) and interpreted them. The author wrote the manuscript. The author presented the publication online at the International Conference on Electronic Government and the Information Systems Perspective in 2020.

VI Second author. The author contributed to the manuscript writing, editing, and commenting. The author provided guidance on the aspects related to trust in the context of e-government.

VII Third author. The author contributed to the manuscript compiling, writing, editing and commenting. The author provided guidance on the electronic identity and trust aspects mentioned in the publication. The author presented the publication at the Conference on e-Business, e-Services,and e-Society in Trondheim, Norway in 2019.

VIII Third author. The publication was initially submitted as a master's thesis by the first author who in turn was co-supervised by the author). The publication was commented, edited and complemented by the author. The author provided guidance on the manuscript writing to the first author of the publication.

IX Third author. The publication was initially submitted as a master's thesis. The author restructured the thesis into a journal article, complemented with additional literature review, and edited the manuscript. The author also handled several rounds of revision introducing changes together with the second and fourth authors. The publication was awarded as the Research Article of the Year 2021 in the School of Information Technologies at Tallinn University of Technology.

Abbreviations

ANT	Actor Network Theory
CA	Certification Authority
CEO	Chief Executive Officer
CTO	Chief Technology Officer
DOI	Diffusion of Innovation Theory
eID	Electronic Identity
eIDAS	Electronic IDentification, Authentication, and trust Services
eGA	e-Governance Academy
EU	European Union
ID	Identity Document
IS	Information Systems
OCSP	Online Certificate Status Protocol
PBGV	Police and Border Guard Board
PIN	Personal Identification Number
PKI	Public Key Infrastructure
SLR	Systematic Literature Review
TAM	Technology Acceptance Theories' abbreviations
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
QDA	Qualitative Data Analysis
RIA	Riigi Infosüsteemi Amet (State Information Systems Authority)
RQ	Research Question
SK	Sertifitseerimiskeskus (Certification Center)
UTAUT	Unified Theory of Acceptance and Use of Technology

1 Introduction

The aim of this dissertation is to unfold and examine how and why public acceptance of electronic identity impacts the success of e-government. It is widely known that electronic identity (further, eID) is one of the pillars that support e-government [27], [I,III,VI]. eID serves as a key to open the access to e-services. Ever since eID has been introduced into national identity management, an enormous amount of theoretical and practical knowledge accumulated. Going through different domains of eID, such as, technology behind it, policy field, legal framework, economic aspect, and eID adoption and acceptance, the last one has caught our attention, as we discovered a knowledge gap in the end-user perspective of eID.

According to the World Bank Group, eID is crucial for the government's ability to deliver services to its citizens while actually knowing who those people are and their attributes [6]. eID also supports the development of private sector and facilitates their service delivery processes through providing trustworthy ID credentials to citizens, i.e., private sector's customers. Lastly, the World Bank Organization highlights the role of eID in growing the digital economy and enhancing regional and global integration. eID is needed for secure identification and authentication, and is linked with digital signatures and trust services. Together, they enable faster digital connections and transactions among people, governments, organizations, and commercial platforms through information, data, and cash flow. *Ibid.*

As we are based in Estonia, one of the most advanced digital societies with a well-functioning and mature eID [76, 66, 85, 77, 47], a decision to take the country as the scene for examining eID acceptance was made.

While this dissertation consolidates results of a four-year-long research journey through the end-user perspective of eID in attempt to emphasize its impact and role in a larger picture of a digital state and society, we also provide to the readers the view from the backstage of a decision-making process that has been taking place all these years in order to achieve the current level of e-Estonia's development and its e-society. We examine the user's perceptions and opinions about eID and at the same time we speak to practitioners and first-hand experts who have created and been maintaining eID ever since.

This dissertation will interest a wide audience that includes public sector officials, entrepreneurs, identity providers, independent practitioners, academicians, and digital society enthusiasts who are keen to find out more about electronic identity. All the named groups of people will be able to gain insights relevant to their fields of expertise. As we use scientific inquiry, tools and theories to investigate public acceptance of eID, our research journey eventually leads us to examining not only abstract concepts and ideas but also actions, decisions, and strategies of those who facilitated the eID to reach the end-users and integrate it as part of the e-government ecosystem.

Through a single case study with embedded units of analysis, we study how public acceptance of eID is reflected in other researchers' work, we use the derived factors to examine Estonian citizens' perceptions of and attitudes towards eID, and we analyze the top experts' opinions on eID public acceptance and its importance to the overall success of e-Government in Estonia. As we answer the research questions, we come up with a generalized view on eID public acceptance by means of institutional design framework [64].

It is important to discuss the subtlety of the term "public acceptance" and clarify its usage in this dissertation. Are *technology acceptance* and *public acceptance* the same? While eID is usually rather perceived as a technical artifact, the objective of this dissertation goes beyond the "technology acceptance" of eID. Classically, investigations in technology acceptance treat the acceptance of a technical artifact or measure in the context of an organization; typically, with the aim to understand the value added to the workflows of the organization. Such treatment of technology acceptance is too narrow for the purpose of this dissertation. eID belongs to complex, large-scale information system landscapes such as e-government ecosystems that in turn presupposes continuous processes of communication between all stakeholders. In the context of technology acceptance, one of these stakeholders is the end user, i.e., the eventual beneficiary of the system. Therefore, the norms and circumstances in which end users function also dictate their roles. Susanto and Aljoza state that "e-Government users are more than just technology users" [113]. The researchers identify three roles: *technology users*, *citizens*, and *customers*. Depending on the role, different factors may affect the acceptance and the process of adoption. Within this dissertation, the accent is placed primarily on the role of citizens together with conditions and factors that determine and lead to acceptance. Hence, this crucial aspect defines what makes the context of "public acceptance" being "public" in this dissertation.

In the context of e-governance, e-government, and eID, a concept of "public acceptance" is more suitable. The term of "technology acceptance" is, in our opinion, too specific according to its usual context of use, i.e., the organizational setting, and at the same time not specific enough when it comes to the range of phenomena to be investigated in the domain of eID acceptance. Therefore, applying technology acceptance analysis in a straightforward manner within this research (with its set aims and objectives), would bear the risk the domain-specific factors to be excluded or overlooked. In contrast, the concept of "public acceptance", as we want to use it in this dissertation, includes the investigation of aspects that concern (i) the specific roles that users take, (ii) the continuous relationships of users with providers of eID solutions, and (iii) the environment in which users and providers function and interact.

The importance of public acceptance towards technologies, particularly, e-government, has been receiving attention from scholars over the years considering the rising number of publications dedicated to this topic [53, 13, 86]. At the same time, despite the vast interest in the topic, there is still no clear definition of this concept. In the context of technologies, Vlassenroot et al. attempt to define it as a *"[...] phenomenon, how potential users will react and act if a certain measure or device is implemented"* [132].

Therefore, taking Estonia as the context country, we study the phenomenon of eID public acceptance by answering three research questions:

- *RQ1 What are the factors that impact eID public acceptance?* We conduct the very first systematic literature review (SLR) that examines existing research on national electronic identity systems that focus on the end-users, and first of all, the citizens. We collect a range of research work that points out to various aspects acknowledged as important from the user perspective and those that have direct impact on the eID public acceptance. We organize the significant aspects into 12 categories, i.e., factors.

- *RQ2 How do citizens perceive eID?* 99% of the Estonian population have ID cards. Two thirds of the Estonian population use eID on a regular basis which also includes other means of electronic identity. Considering the maturity of eID, its technical architecture and legal framework, we pose this research question to reveal the actual perceptions and attitudes from the end-users themselves. To answer this research question, we conduct a questionnaire designed on the basis of previously derived factors of eID public acceptance. We tailor the questions for the Estonian eID, i.e., we maintain details and peculiarities of the national eID scheme so that we receive a deeper understanding of the country's case.

- *RQ3 How does eID public acceptance impact the success of national e-governance initiatives?* To validate the findings of previous studies and contextualize them, we conduct seven in-depth expert interviews with the top specialists in the eID and e-government field who eyewitnessed and participated throughout the entire development path. We seek explanations on why people adopting the solutions is important for a digital state. Therefore, we ask experts to share their opinion and vision of how people's acceptance of eID influenced the current state of eID maturity. To help interpret the big picture and see how eID public acceptance facilitates e-government, we use institutional design framework from Koppenjan and Groenewegen [64].

The reader will be able to go through this dissertation page-by-page to familiarize with the following: a) what public acceptance of eID is (current Chapter); b) what three research questions about eID public acceptance will be investigated (current Chapter); c) what methods we used and why to guide us in answering the posed questions (Chapter 2); d) which theories we use to explain and interpret the phenomenon of public acceptance; e) what background and context Estonian eID has and why it matters (Chapter 4); f) our results and answers to research questions (Chapter 5); g) our contemplation and discussion of the findings we obtained (Chapter 6); and lastly, h) the conclusion with which we finalize our work (Chapter 7).

2 Research Methodology

This chapter provides an overview of the research approach and the research methods that we used within this dissertation. A thorough description and justification of the chosen methodology and the protocols we followed to process our data is aimed to navigate the reader through the body of our work and understand the chain of presented results and arguments, their structure and implications.

The goal of our research efforts is to explain the phenomenon of eID public acceptance and to provide a detailed analysis of aspects and auxiliary elements that it contains.

The research of this dissertation is conducted primarily in the tradition of interpretivism [78]. According to interpretivist research philosophy, the reality, as well as knowledge about it (both society's and researcher's), is "incapable of being understood independent of the social actors" [91]. Here, interpretivism ties together with constructivism. A social research approach that is oriented towards constructivism would be inherently qualitative, as it would embrace constructivist viewpoints such that individuals seek understanding of the world in which they live and work [42] through their very own experience of the world in which they live and work ("*The unexamined life is not worth living*" Socrates). Hence, a constructivist research approach would demand that the reality is explained through subjective views, beliefs, and opinions, i.e., social constructs. Since there are multiple meanings and views, the researchers' task is then to look into the complexity of these views, rather than attempting to place them in narrow categories. What matters here is relying, as much as possible, on the participants' observations and perceptions of the studied situation [42]. As a consequence, an important advantage of the interpretivist approach is that "researchers can not only describe objects, human or events, but also deeply understand them in social context" [67]. Interpretivism is concerned with studying the processes of individuals' interactions and specific contexts in which these interactions take place. Therefore, the interpretivist approach serves best in studying complex socio-technical phenomena such as e-governance, eID and public acceptance of eID.

Predominant research approaches that are in line with interpretivism are case studies and field studies [91]. It is worth to mention that in case of interpretivism, case studies are usually conducted preferably by utilizing an inductive rather than a deductive approach, which means that there is no definite theory as starting point; instead, the research is about generating a theory, inductively developing it by identifying patterns of meaning throughout the research process [41]. The research of this dissertation has been conducted as case study research. In [26], Benbasat et al. state: "a case study examines a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations). "In the so far latest edition of his book [139], Robert Yin provides the following definition of a case study: "A case study is an empirical method that investigates a contemporary phenomenon (the 'case') in depth and in a real-world context, especially when boundaries between phenomenon and context may not be clearly evident." An important feature of case studies that makes this method particularly appropriate for this dissertation is their reliance on "multiple sources of evidence, with data deeding to converge in a triangulation fashion." [139]

Case study research is a suitable methodology when an in-depth focus on a case is needed while keeping a holistic and real-world perspective in studying social phenomena at different scales, for example, ranging from small groups' behaviours over managerial and organisational processes to maturation of whole industries or domains [139]. It is also a preferred method if the researcher aims to explain phenomena, i.e., seeks to answer

Table 1: "Key Characteristics of Case Studies" [26]. The table is entirely taken from [26], p. 371.

1. Phenomenon is examined in a natural setting.
2. Data are collected by multiple means.
3. One or few entities (person, group, or organization) are examined.
4. The complexity of the unit is studied intensively.
5. Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration.
6. No experimental controls or manipulation are involved.
7. The investigator may not specify the set of independent and dependent variables in advance.
8. The results derived depend heavily on the integrative powers of the investigator.
9. Changes in site selection and data collection methods could take place as the investigator develops new hypotheses.
10. Case research is useful in the study of "why" and "how" questions because these with operational links to be traced over time rather than with frequency or incidence.
11. The focus is on contemporary events.

"how" and "why" questions. Furthermore, case studies make sense if the phenomenon under investigation takes place in the present and requires "an extensive and 'in-depth' description." [139]. Usually, the phenomenon itself does not have clearly evident boundaries and no experiments or manipulations are used to intervene the natural course of events [26]. Within the information systems (IS) domain, case studies contrast with other common approaches in so far that, prior to the study, the researcher usually possesses less knowledge of the variables he is interested in and how they will be measured [26]. At the same time, Benbasat et al. emphasize [26] that the degree of this knowledge may still vary depending on the units of analysis, their number, and whether they are compared with each other. In [26], Benbasat et al. compiled eleven "key characteristics of case studies" [26] from [25, 29, 61, 112, 138] that can also serve as criteria for determining the suitability of the case study research method for a concrete research endeavour, see Table 1.

Jennifer Platt, a representative of American methodological thought, has examined the limited and rather isolated applications of case studies in only certain research problems in the past; and in the early 1990s, she concluded that the case study has increasingly been treated as method that has its own "logic of design [. . .] a strategy to be preferred when circumstances and research problems are appropriate rather than an ideological commitment to be followed whatever the circumstances." [100]. Therefore, considering the identified research questions, research problem and objectives together with the scope of research (see Chapter 1), we applied the given methodological approach.

In accordance with Table 1, we have compiled Table 2 that analyzes in how far our research endeavours shows the key characteristics of case study research of [26], in order to demonstrate the suitability of the given method for our research.

Table 2: Key characteristics of our research endeavours according to [26], compare with Table 1.

Criterion	Explanation
1. The phenomenon is investigated in its natural setting	The subject of eID public acceptance is studied in its natural setting. This is dictated by the nature of the phenomenon itself, i.e., it is a phenomenon how users (citizens) react and act if a solution (eID) will be implemented. As the eID in Estonia is state-provided, studying the phenomenon of public acceptance in an artificial setting and attempting to replicate real-life conditions would contradict with the essence and definition of the notion itself.
2. Data are collected by multiple means.	Desk research, surveys, questionnaires, and expert interviews are used within this research. The data is further triangulated
3. One or few entities are examined	In our case, the investigated eID ecosystem involves a large number of stakeholders amongst which are individuals, groups, organizations, systems, abstract notions, etc. Therefore, we incorporate quantitative/qualitative survey techniques into our research methodology
4. The complexity of the unit is studied intensively	This case study consists of one unit of analysis, which is the country of Estonia. The unit is investigated thoroughly and in detail since in the context of public acceptance, the country as a unit can be divided in multiple subunits or embedded units.
5. Exploratory stage of research	The idea, that case study research is more suitable for exploratory research, is a rather classical viewpoint. We follow Robert Yin [139] who considers case study research as beneficial for both exploratory, descriptive and explanatory research efforts. This research is not located in its exploratory phase. We argue that due to the wide and exhaustive body of knowledge on eID and the Estonian eID, the goal is to use this existing knowledge to focus on a particular fragment, i.e., the phenomenon of eID public acceptance. By means of topic-specific data collection, an explanatory inquiry was carried out.
6. No experimental controls or manipulation are involved	No experiments were designed or conducted within this research.
7. The investigator may not specify the set of independent and dependent variables in advance	No specific variables were identified in advance, nor this was a priority or goal within this research. It is possible to conceive that public acceptance can be posited as the dependent variable, however, the design of this research does not presuppose any experiments or measurement.
8. The results derived depend heavily on the integrative powers of the investigator	The results of this work should be reviewed and assessed by other researchers and experts of the field.

Continued on next page

Table 2 – continued from previous page

Criterion	Explanation
9. Changes in site selection and data collection methods could take place as the investigator develops new hypotheses.	As the research presented in this dissertation was conducted over four years, both the site selection and the data collection methods were modified together with the focus and objective of this research under the internal and external circumstances
10. Case research is useful in the study of "why" and "how" questions because these with operational links to be traced over time rather than with frequency or incidence	Two out of three research questions are "how" questions. In order to provide answers to these questions, an investigation of facts and events occurring within a certain period of time was required. Indeed, the focus was placed on the "quality" of those occurrences rather than on their frequency or whether they occurred in general.
11. The focus is on contemporary events	The main focus of the research was placed on the public acceptance of eID which can be seen as both a process that takes time, but also a result or an outcome, and hence may require investigating preceding events and actions). According to [139], "case studies are preferred when the relevant behaviours still cannot be manipulated and when the desire is to study some contemporary event of set of events ('contemporary' meaning a fluid rendition of the recent past and the present, not just the present".

Yin [139] distinguishes several types of case studies. He claims that there was a tendency among many social researchers to array research methods hierarchically: case studies were suitable only as a tool within the exploratory phase of research; histories and surveys for the descriptive phase; and only experiments could be used for explanatory purposes. Yin, however, does not agree with the idea that a case study is only suitable for the preliminary phase of an inquiry and he rejects such hierarchy by pointing out that many of the most prominent case studies have been explanatory case studies, e.g., "Essence of Decision: Explaining the Cuban Missile Crisis" by Allison and Zelikow [18]. A similar misconception can be refuted for descriptive case studies, which aside from history can be found in other major branches of science such as political science and sociology. Yin claims [139] that every research method can be applied in each scenario, be it explanatory, descriptive, or exploratory. And even then, the sharp boundaries between the inquiries are not necessarily implied since there are many overlaps between albeit distinct characteristics of each. Indeed, the form of a question may already give a hint of which research method thus is appropriate. However, Yin prompts to select first those inquiry and method that will be most advantageous within the conducted research.

2.1 Research Design

According to Yin [139], a case study can be a holistic case study, where the case is studied as a whole; whereas an embedded case consists of several units of analysis.

For the purpose of this dissertation, an embedded case study design is introduced. This decision was taken since the original case study has expanded and evolved over time.

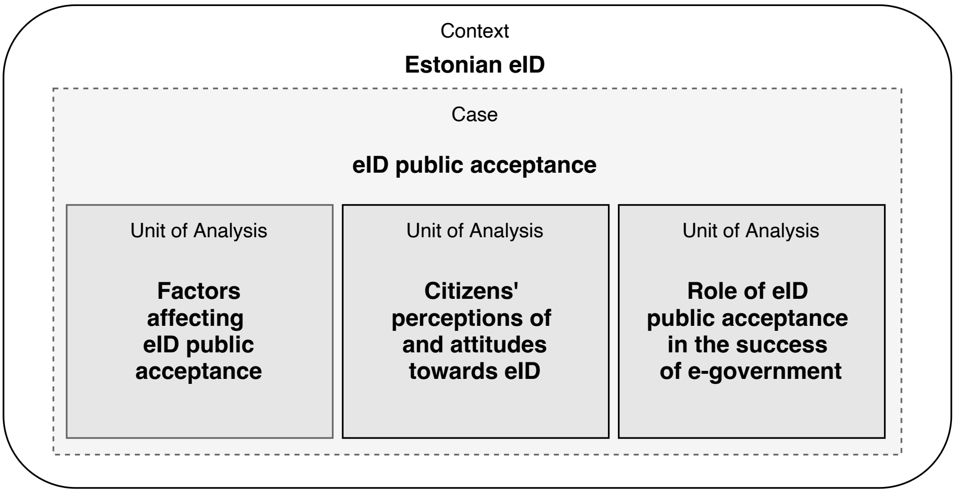

Context
Estonian eID
Case
eID public acceptance
Unit of Analysis
Factors affecting eID public acceptance
Unit of Analysis
Citizens' perceptions of and attitudes towards eID
Unit of Analysis
Role of eID public acceptance in the success of e-government

Figure 1: Case study design.

While collecting the data, the orientation of the study shifted. At the same time, the initially planned exploratory investigation has evolved into an explanatory. In the preliminary stage, where the preparations for the research took place, i.e., learning countries' practices and identifying the knowledge gap in the literature, the types of asked questions were "what" and "which". However, once the data accumulated, it became clear, that the focus needs to be changed, and therefore, the boundaries of the case were limited to a specific case, i.e., the public acceptance of eID within the context of a particular country, Estonia, and its eID system. To avoid a too abstract level of study, the initially planned comparative multiple case study design, in which several countries would have been examined, was replaced in favor of a single embedded case study design. Acknowledging this shift, in fact, allowed for this work to attain a clear focus on a particular case in a particular context.

In order to design a case study that allows for various insights and discoveries, subunits are useful tools for maintaining the focus. To achieve this, the subunits need be identified and aligned according to the research questions. Within this dissertation, the units of analysis also fulfill the function of streamlining the outcomes into the "larger" unit, i.e., the "case". In other words, these units help to define the public acceptance in Estonia. This not only helps to increase the clarity of the research design, but also addresses the risk of introducing a subunit in a case in general. Often, determining the type of a case study (exploratory, descriptive, explanatory) is, to a large extent, a matter of perspective. Also, different units of analysis inside a case study represent different types of inquiries. Within the research of this dissertation, the types of inquiry are determined for each unit of analysis together with the overall emphasis on the explanatory nature of this case study (see Figure 1).

The general analysis strategy for the case study presented in the given dissertation relies on a combination of two analytical techniques, i.e., linking data to theoretical propositions and examining rival explanations. The theoretical propositions are expressed through the theoretical framework presented in Chapter 2 that will provide the necessary concepts, notions, specifications and linkages to build up the case and interpret its findings. Rival explanations, abundantly discussed by Yin [139], serve as one of the criteria for evaluating the strength of findings, as they are also crucial for both internal and external va-

Table 3: Case study design.

Unit of Analysis	**Type of inquiry**
1. *Factors affecting eID public acceptance* The RQ 1 which corresponds with this unit of analysis is answered via a systematic literature review (SLR) [III] and in-depth expert interviews. The nature of inquiry for this question was initially exploratory as this was the inception phase of the research. The purpose of this question is to identify factors of public/user acceptance specific to eID by means of SLR. The input from the SLR has served as a part of the theoretical framework in the further activities in other research block s. Furthermore, the outcomes were later used to reiterate the findings for RQ1 through triangulation.	Exploratory/Explanatory
2. *Citizens perceptions of and attitudes towards eID* The RQ2 that corresponds with this unit of analysis aims to analyze Estonian citizens' perceptions of and attitudes towards eID. A user-centric approach is crucial when introducing a new system or solution, hence, a detailed analysis of user needs is required. Here, using the input from the previously conducted SLR, a questionnaire was specifically designed to find out i) what qualities and features of the current authentication options in Estonia the citizens find un- and appealing, and ii) what general tendencies in the public's narrative are in the context of eID [IV,V]. RQ2 was also partially addressed by the analysis on citizens' perspectives on eID presented in [I]. It gained a series of valuable insights from in-depth expert interviews that provided the stakeholders' perspective on eID public acceptance.	Explanatory
3. *Role of eID public acceptance in the success of e-government* The RQ3 that corresponds to this unit of analysis addresses the inquiry on the significance of eID public acceptance in the overall success of e-governance in Estonia. It provides views of stakeholders on the subject of study in order to understand how Estonia reached the current level of eID acceptance among its users and whether it is important in the state's endeavors in implementing and maintaining a digital government. In-depth expert interviews with top experts from relevant fields were conducted and analyzed. The outcome complemented the previously acquired results and enriched the case evidences with experts' opinions.	Explanatory

lidity of a case study by means of introducing alternative plausible explanations for the outcomes.

2.2 Timeline, Data Sources and Data Collection Procedures

The data for this dissertation comprises several rounds of data collection by means of multiple methods from a wide range of data sources.

The central methods for data collection within this case study are in-depth expert interviews and questionnaires. Additionally, a systematic literature review and desk research have been conducted.

Semi-structured in-depth expert interviews were used as one of the tools for collecting qualitative data. An interview can provide are that open-ended questions and probes "yield in-depth responses about people's experiences, perceptions, opinions, feelings, and knowledge". The amount of context is sufficient for interpretation.

Along with interviews, online qualitative surveys were used to collect both quantitative and qualitative data, as these surveys combined the use of close- and open-ended questions. It is quite common to regard surveys mostly as a tool for collecting quantitative data. However, Braun et al. are convinced [32] that qualitative surveys can serve as a rich source of qualitative data with a potential to harness new perspectives and in-depth understanding of investigated matters. In [32], Braun et al. highlight a number of advantages that characterize online qualitative surveys. Firstly, the method offers flexibility and openness in addressing an array of research questions through the access to a wide range of data that can include views, experiences, or material practices [32]. Secondly, online qualitative surveys are affordable to organize and facilitate easy access to populations of different sizes that may often be spread geographically. Additionally, the aim of a qualitative survey is to collect in-depth insights about the topic of research interest [32]. Another advantage of qualitative surveys is the anonymous mode of data collection as it usually encourages the respondents to disclose (more) information of the surveyed topic. One of the concerns around this method is the claim that as compared to interviews, within surveys there is a high risk of losing depth of data. Yet, Braun et al. refute this argument [32] by providing a range of research examples that demonstrate that written responses can offer a great deal of details within just even one submitted response. Such responses may often provide far more relevant information with a strong focus on the subject than interviews which may be less effective in case the informant tells a "bloated story" from which its meaning cannot be grasped easily or, on contrary, the informant's answer is too parsimonious. Either way, independent of the method, these risks are real also because of circumstances and/or researcher's skills.

Within the current dissertation, the surveys are split in two data collection rounds described below and consist, as was already mentioned, of close- and open-ended questions. Though compelling arguments in favor of fully qualitative online surveys are brought above, we also introduced questions with prepared multiple-choice answers in order to collect quantitative data as well. Combining qualitative and quantitative data has acquired a wider acceptance and employment as a research practice across different research fields [73]. The aim of mixed method data collection is to complement the insights that each has to offer.

Another data collection method used within this dissertation is literature review.

Conducted and published in 2019, the literature review in the context of this dissertation serves as one of the research methods for data collection. Not only it performs the common function of providing an overview of a particular research area on eID and public acceptance, but it also synthesizes research findings to uncover research gaps that in turn urge for creating new theoretical concepts and models [111].

Keeping in mind the purpose of this literature review, it was conducted following the systematic literature review guidelines of Kitchenham and Charters [63] (widely known as Kitchenham's guidelines). According to Moher et al., a systematic literature review helps "to identify all empirical evidence that fits the pre-specified inclusion criteria to answer a particular research question or hypothesis. By using explicit and systematic methods when reviewing articles and all available evidence, bias can be minimized, thus providing reliable findings from which conclusions can be drawn and decisions made" [84]. Kitchenham's guidelines increased the rigor and trustworthiness of the conducted study. This way, the adhered SLR protocol allowed to extract a set of categories that group factors influencing eID acceptance. These factors were later incorporated into further research activities as a part of theoretical framework.

The data sources and data collection procedures are further described in a form of a timeline which increases the clarity and understanding of the dissertation's research design and interrelations between its components.

The first round of data collection took place in 2017 [I]. The research objective of the study was to examine the status of eID adoption in Ukraine, evaluate the citizens' awareness level and identify its associated drivers and barriers. The study employed an exploratory type of inquire. The data were collected primarily by means of online surveys that were launched among citizens and yielded 222 responses. The goal of the survey was to analyze how aware citizens are about the back then newly introduced eID, whether and how often they use e-services, and what are the overall attitudes towards the digitalizing government. Though this study is mainly citizen-centric when it comes to the data source, in order to acquire a broader view on the problem of eID awareness, three expert interviews with public officials were conducted. All three interviewees represent the stakeholders of a local government project on an issuance of a citizen card with multiple functions and applications. The interviews were semi-structured, consisted of ten initial questions. The interviews lasted on average 45 minutes and were recorded with a desktop audio application. The codes and themes were created using excel sheets and analyzed manually to address the overall research question on the eID public awareness and its role in the success of eID implementation. Along with primary data collection techniques, a desk research was also conducted with the purpose of learning international practices of eID implementation and introduction.

The work [I] has served as a commencement for the current case study and identified the topic of public acceptance as a point of our interest. The outcomes of this study will be incorporated to address the research questions of this dissertation (see Section 5.1).

The second data collection round took place in 2018. A literature review employing SLR guidelines and procedures was conducted [III]. Adhering to [63] and [133], the literature review included the next steps:

1. Identifying the need for literature review.
2. Formulation the research question.
3. Developing a search strategy.
4. Carrying out a comprehensive search of studies.
5. Analyzing and extracting data from the selected studies.
6. Synthesizing the results

7. Writing-up an interpretation of results.

The search terms were adapted to answer the following research question: what are the factors that affect eID public acceptance?

The search has retrieved in total 146 studies, out of which, after careful consideration of the subject, 39 studies were included into the final set of review. Among the retrieved studies, such types as conference proceedings, journal articles, book chapters, theses, policy documents, and reports were captured.

Next, the relevant studies were processed and arranged in a set of categories that represent factors of eID public acceptance and consist of operational notions used and accommodated further within the current case study research. Thus, the conducted study [III] serves as a part of theoretical framework for the current case study research. It also represents a wide array of related work on eID acceptance.

The third round of data collection took place in 2019. The study was design as a case study research with a semi-structured qualitative online survey as the main data collection method. The survey comprised closed and open-ended questions. The latter were analysed by means of thematic analysis that was conducted manually and facilitated by excel sheets. The pre-defined constructs, i.e., the factors of eID public acceptance, as the outcome of the second data collection round serve as a theoretical framework to conceptualize and interpret the results of the survey.

Comparing to the second study, the investigated issue at hand was now narrower. The aim of the study was to look in the case of Estonia when it comes to the daily use of eID and its multiple means of authentication. The research questions for this study were posed as follows:

1. Which eID authentication methods are preferred by the citizens?
2. What are the factors of eID public acceptance in Estonia?

The survey was designed for the owners of the Estonian eID, which includes citizens, residents, individuals holding a digital citizenship (e-residency), holders of electronic identity cards. Altogether, the survey yielded n = 268 responses (the population of Estonia is approximately 1,328,000 citizen, and approximately.= 97% of Estonian citizens have an eID [21], which is approximately N = 1.288.000, resulting in 95% confidence level with 6% margin). The survey was created by means of an online platform surveymonkey.com. Social media platforms and email channels were used to distribute the survey. As Estonia is a multi-lingual country, the survey was distributed in three languages: Estonian, Russian, and English. The survey consisted of 12 questions.

Additionally, official requests for data provision were submitted to the issuer of eID, Police Border Guard Board (PBGB), and the trust services provider, SK ID Solutions AS (SK). These institutions were able to provide statistical data on the total number of Online Certificate Status Protocol (OCSP) requests, the number of national eID part of the OCSP requests (all national documents including mobile-ID), mobile ID and Smart ID usage in numbers within the period of 01.01.2017–01.05.2019. This data was used to complement the analysis of the survey responses (see Figure 10).

The fourth round of data collection took place in 2021 in a form of in-depth expert interviews. The primary goal of the interviews was to answer RQ3, however, based on the outcomes and insights from previous studies, the interview questions were formulated to address also the RQ1 and RQ2. In total, seven in-depth interviews with top experts from the eID domain were conducted. Table 4 presents the positions and affiliations of the expert interviews as well as the duration of the interviews. To ensure data privacy

Table 4: List of interviewees.

	Position	Affiliation
1.	Director	eGovernance Academy (eGA)
2.	CEO	Non-profit organization
3.	CEO	SK ID solutions
4.	Government CTO	Ministry of Economic Affairs and Communication
5.	Deputy Director	State Information System Authority (RIA)
6.	Head of eID Department	State Information System Authority (RIA)
7.	Founder of eGA, Consultant	Independent

and ethical concerns, prior informed consent was obtained from each of the interviewees before the interview process. The interviews were recorded via Microsoft Teams that has also allowed to use the screen sharing functionality which helped to display the interview questions for the informants. This in turn ensured staying on track with the narratives but also allowed focusing on each question one-by-one while having the possibility to be flexible and detour for the emerging questions and then circle back.

The steps taken within the interview process are:

1. Designing interview questions based on the RQ and prior results.
2. Designing an interview guide.
3. Conducting video-recorded interviews.
4. Transcribing recordings of the interviews.
5. Analyzing collected data.

Six out of seven interviews took place online vis Microsoft Teams and were recorded by means of software functionalities. The interviews were transcribed by means of a web-based software Otter.ai.

In order to ensure a high quality of data for further analysis, and for the purposes of transcriptions, a transcription protocol was designed. The protocol and its overall structure took into account the seven principles of audio transcription suggested by Mergenthaler and Stinson [82]. The principles are displayed as follows:

1. Preserve the morphologic naturalness of transcription. Keep word forms, the form of commentaries, and the use of punctuation as close as possible to speech presentation and consistent with what is typically acceptable in writ-ten text.
2. Preserve the naturalness of the transcript structure. Keep text clearly structured by speech markers (i.e., like printed versions of plays or movie scripts).
3. The transcript should be an exact reproduction. Generate a verbatim account. Do not prematurely reduce text.
4. The transcription rules should be universal. Make transcripts suitable for both human/researcher and computer use.
5. The transcription rules should be complete. Transcribers should require only these rules to prepare transcripts. Everyday language competence rather than specific knowledge (e.g., linguistic theories) should be required.

6. The transcription rules should be independent. Transcription standards should be independent of transcribers as well as understandable and applicable by researchers or third parties.

7. The transcription rules should be intellectually elegant. Keep rules limited in number, simple, and easy to learn. Guided by the above principles, the transcription protocol for current study was also using directions provided by McLellan et al. in [80]. A few steps of the original transcription protocol were omitted as the software automatically completed them.

In line with the work of McLellan et al. [80], the next steps were applied to the recordings:

- The recordings were transcribed verbatim (i.e., recorded word for word, exactly as said), but excluding any nonverbal and background sounds in order to facilitate the thematic in NVivo 12.
- Nonverbal sounds were excluded from the transripts.
- If interviewers or interviewees mispronounced words, these words were transcribed as the individual said them.
- The transcript were "cleaned up" by removing foul language, slang, grammatical errors, or misuse of words or concepts. If an incorrect or unexpected pronunciation resulted in difficulties with comprehension of the text, the correct word was corrected.
- The spelling of key words, blended or compound words, common phrases, and identifiers were standardized across all individual transcripts. Enunciated reductions (e.g., gotta, kinda, lotta, sorta, wanna, coulda, could've, couldn't, coudn've, would've, wouldn't, wouldn've, should've, shouldn't, shouldn've) plus standard contractions of is, am, are, had, have, would, and whatnot were used.
- Filler words (such as "huh", "mm", "mhm", "yeah") were transcribed.
- Word or phrase repetitions were transcribed. If a word was cut off or truncated, a hyphen was inserted at the end of the last letter or audible sound.

The Otter.ai software identified portions of the recording that are inaudible or difficult to recognize. If a relatively small segment of the recording (a word or short sentence) was partially unintelligible, we typed the phrase "inaudible." This information was placed in square brackets.

We checked (proofread) all transcriptions against the recording and revise the transcript file accordingly. We adopted a "three-pass-per-tape" policy whereby each recording was listened to three times against the transcript before it was exported.

This scrupulous procedure aims to provide a deep level of transcription that is required to correspond with the intended level of analysis of our work. In [80], McLellan et al. argue that "If an analysis focuses on providing an in-depth description of the knowledge, attitudes, values, beliefs, or experiences of an individual, a group of individuals, or groups of individuals, a greater number and possibly lengthier units of text need to be included in the transcript. With this type of analysis, researchers are not only interested in identifying patterns and salient themes. They also want to demonstrate variations in how social phenomena are framed, articulated, and experienced as well as the relationships within and

Table 5: Interview length.

Interview	Words	Pages, A4	Duration
Informant 1	6,800	13	0:58:00
Informant 2	9,240	16	1:02:00
Informant 3	7,765	14	1:08:00
Informant 4	8,716	13	1:00:00
Informant 5	4,609	12	0:42:00
Informant 6	1,1732	17	1:25:00
Informant 7	7,144	11	1:20:00
Total	*5̃,6000*	*9̃6*	*7̃:58:00*

between particular elements of such phenomena." In [28], Boguraev et al. also suggest that "[...] granularity of analysis" must be closely tied into context and rely on linguistic phrases".

The transcription of all interviews for the current study yielded is presented in numbers in Table 5. The numbers are approximate representations as, for example, the number of pages may vary depending on the formatting of the document. In case of the given transcriptions, the number of pages is a result of such formatting parameters as: font Arial, 12 pt, 1.15 interval.

The transcripts were then uploaded to the qualitative data analysis software NVivo 12.

The full description of the thematic analysis procedures is provided in Section 2.3. The analysis procedure conducted for all four data collection rounds within the current dissertation consists of the next stages.

To explain the analysis procedure, it is worth mentioning again that topic itself has unfolded over time, and each following data collection round was conducted with consideration of the analysis outcomes from previous ones. As such, the research questions posed in each study and answered in the form of results that were also published earlier [I,III,IV]Tsap20Tsap20b cannot serve as a standalone answer(s) for the research question(s) in the context of the current dissertation. Referring to the current case study design, the research questions in the studies belong to corresponding units of analysis. Each of those, in isolation, do provide answers for the questions within them. In chronological perspective, the units of analysis are linked to each other. However, only in the context of the entire case, the value produced by each unit added up altogether can provide a synergic result that in turn addresses the overarching research questions. Therefore, all results will be evaluated using triangulation. Moreover, they will be interpreted through and opposed to the theoretical concepts brought in Chapter 2. Explanation building technique and rival explanations discussed by Yin [139] will be used to build and test the narrative.

2.3 Thematic Analysis

Thematic analysis is a prevailing analysis method in the current dissertation. Thematic analysis is argued to be one of the foundational methods for conducting qualitative analysis [31]. Boyatzis [30] defines it rather as a tool that can be used across various methods. He also believes that this is one of the generic techniques applied within qualitative inquiry. However, Braun and Clarke [31] insist on thematic analysis to be considered as an independent, stand-alone method.

Thematic analysis is valued for its flexibility. This method can be applied across theoretical and epistemological approaches while other methods belong either to essentialist or constructionist paradigms. In the opinion of Braun and Clarke [31] “through its theoretical freedom, thematic analysis provides a flexible and useful research tool, which can potentially provide a rich and detailed, yet complex, account of data”.

Throughout the first, second, and third data collection rounds, thematic analysis was used as a complementary analysis method, which was justified by a relatively small amount of data.

In the first data collection round [I], thematic analysis was used to analyze and interpret open-ended questions in the questionnaire and identify main themes in the three expert interviews. In this round, the thematic analysis was conducted manually using Excel sheets and employed a fully inductive approach in determining main themes.

In the second data collection round [III], thematic analysis was used to synthesize and structure the results of the literature review and consisted of two phases. The first phase took place once the final set of documents was retrieved and each item has gone through a thorough read and identifying relevant narratives marked as codes in the item files. After several rounds of reading the identified fragments, or codes, categories, i.e., the factors of eID public acceptance, were formulated, which in other terms were also the themes. Here, the first phase employed an inductive approach allowing to rely on data while identifying the codes and themes. Further, as a part of the second phase of thematic analysis, the identified codes were interpreted against the created set of measures aimed at determining whether the code, or the notion that underlies in of the factors, we highlighted as a positive, negative, binary, or neutral notion/instance. Here, in contrast with the first phase, a deductive approach was applied when determining the codes and relations between them according to pre-defined categories and measures (see Figure 8).

In the third data collection round [IV,V], as in the first one, thematic analysis was applied in interpreting the open-ended questions’ responses. It proved to be a suitable method due to an amount of textual data submitted by the respondents. The analysis was facilitated by Excel sheets. A hybrid approach of combining deductive and inductive coding enabled to recognize the pre-existing themes, i.e., factors of eID acceptance that were identified prior to this, while at the same time, identifying additional themes that did not fit into existing theme set yet revealed valuable input for further analysis and consideration.

The fourth data collection round (see Section 5.4) was focusing purely on gathering qualitative data by means of semi-structured in-depth expert interviews. Considering the volume of transcribed text and the priority of providing a high-quality and detailed rigorous QDA (qualitative data analysis), a computer-based QDA tool, NVivo 12, was used for thematic analysis.

The interviews were analysed using a hybrid approach in coding, i.e., a combination of inductive and deductive coding. As an analysis strategy, it also implies “immersion in the details and specifics of data to discover important patterns, themes, and interrelationships” [96]. In this sense, the identified themes are strongly rooted in the data itself, or, in other words, are data-driven [96]. Such strategy was exactly applied to answer the main research question within the fourth data collection round. While attempting to understand how and why eID public acceptance becomes important for the success of e-governance, no pre-determined concepts or assumptions were made. As Braun and Clarke describe this approach [31], if the data is collected specifically for this research, the themes identified should not be related to or identical with the questions that were asked of the informants. Nor any theoretical agenda is concerned with it. Hence, within the process of coding, the data related to the main research question of the study was not placed in a pre-existing set of codes. However, in parallel, we also conducted a deductive resp. “theoretical” [31] thematic analysis. Aside from the intention to answer the main re-

Table 6: Steps of thematic analysis (Adapted from [31]).

Phase	Description of the Process
Familiarizing yourself with your data	Transcribing data (if necessary), reading and re-reading the data, noting down initial ideas.
Generating initial codes	Coding interesting features of the data in a systematic fashion across the entire data set, collating data relevant to each code.
Searching for themes	Collating codes into potential themes, gathering all data relevant to each potential theme
Reviewing themes	Checking if the themes work in relation to the coded extracts (Level 1) and the entire data set (Level 2), generating a thematic 'map' of the analysis
Defining and naming themes	Ongoing analysis to refine the specifics of each theme, and the overall story the analysis tells, generating clear definitions and names for each theme.
Producing the report	The final opportunity for analysis. Selection of vivid, compelling extract examples, final analysis of selected extracts, relating back of the analysis to the research question and literature, producing a scholarly report of the analysis.

search question about the correlation between eID public acceptance and e-governance success, we had an opportunity to analyse the data realm based on the already acquired findings and genuine theoretical interest for the topic. Particularly, some of the codes and themes that appeared during the coding process match, for example, with the findings from previous studies. At the same time, some codes were clearly contradicting with those, and hence will be further considered during the final data evaluation for dissertation and serve as rival propositions and explanations that way increasing the validity of the case. This was also a great setting to triangulate our findings later.

Considering the source of data in the last data collection round, which is the interviews from seven top experts in the eID field, a combination of two analytical approaches is justified. Other researchers also argue, that when it comes to analysis on practice, adhering to methodological purity becomes rare. Because of the nature of data collected, i.e., interviews, the reasoning of people is in general complex enough to do a pre-determined hypothesis testing while staying open for other emerging aspects during the research activities [96]. The ability to stay creative and adaptable while studying various phenomena is rather beneficial in a real-world setting with ever-changing conditions.

During the entire process of our thematic analysis, we followed the guidelines of Braun and Clarke [31] in order to assure rigor and accuracy (see Table 6).

Before continuing to the results of thematic analysis, an overview of theories and concepts that form the theoretical framework of this dissertation in Chapter 3 together with the case context description in Chapter 4 need to be provided to ensure a complete and well-rounded understanding of the subject and the outcomes yielded. The current chapter merely reveals the methodological approach, procedures, and tools used together with the story behind the course of this research.

2.4 Validity Procedures

The overall concern with the case study research design when it comes to its validity is mainly related to a belief that its findings are not generalizable to any broader level [139]. Yin [139] calls for a need to distinguish the analytic generalization from the statistical generalization.

To avoid possible pitfalls, it is advisable (if not necessary) to rely on multiple sources of data for triangulation purposes. In [96], Patton also points out the rationale behind employing multiple methods and cites Brewer and Hunter [33] who refer to a combination of several methods as "an arsenal of methods that have nonoverlapping weaknesses in addition to their complementary strengths" [33].

Patton also reminds [96] that triangulation may result in showing some differences in the results achieved by the use different methods, however, it points rather to the fact that each type of inquiry may be influenced by various real-world nuances. This implies an opportunity of a deeper insight and understanding of the studied phenomenon and its relationships with different inquiries. Hence, it also demonstrates that triangulation does not necessarily point to an essentially identical yielded outcomes but rather tests for such consistency [96]. Triangulation is only one part of research quality assurance. A commonly agreed on set of validity procedures can be used for a respective assessment. Table 2.4 is adapted from [139] and includes part of validity procedures of widely accepted framework that are relevant to and adhered within the current case study.

Construct validity refers to the identification of correct operational measures for the concepts being studied. There are two ways to ensure construct validity. The first one is to identify a chain of evidence which means it is possible to trace how the researcher has arrived to the conclusions he reached departing from original research questions. The second is to look at the investigated phenomenon from different perspectives by employing multiple data collection techniques. Table 2.4 also indicates a third measure which is reviewing the case study report by key informants, however, taking into account the format of the case study report that is essentially this dissertation, the review as such is postponed. The test of construct validity within the current case study can be done by referring to the timeline of the research and the data collection procedures' description which aids to establish the chain of evidence. The data collected for this case study employs multiple methods of collection having in mind the importance of triangulation.

Internal validity refers to establishing a causal relationship, whereby certain conditions are believed to lead to other conditions, as distinguished from spurious relationships. Internal validity can be a potential weakness of an explanatory case study particularly since, here, the case study is built on inferences. Gibbert (2008) suggests three techniques to address the risk of weak internal validity. These are the: 1) pattern matching – empirically observed patterns should match with the ones found in previous works in different contexts; 2) clear research framework that explains the causal relations between the constructs whose interaction results in the studied phenomenon; and 3) adopting different perspectives on the outcomes through theory triangulation. Yin's suggestions are similar and the applied ones within the current case study can be seen in Table 2.4. The attempt to ensure the internal validity for the current case study research is done by applying all three of the mentioned techniques. The results received from the analysis of empirical evidence are evaluated against the existing body of knowledge for (in)consistency. The research framework is described in detail in the form of a research design. Coming back again to multiplicity of views, triangulation is accounted. When using Yin's terms of ensuring internal validity, pattern matching, explanation building, and rival explanations are applied to challenge the outcomes of the current case study.

Table 7: Validity procedures.

Tests	**Tactic**	**Research phase in which the tactic is addressed**
Construct validity	Use multiple sources of evidence Have key informants review the draft of report	Data collection Composition
Internal validity	Pattern matching Explanation building Address rival explanations	Data analysis
External validity	Use of theory in single-case studies	Research design
Reliability	Use of case study protocol Developing case study database Maintain a chain of evidence	Data collection

External validity refers to showing whether and how a case study's findings can be generalized. The explanatory nature of this case study requires to point out the unique circumstances and setting that might have been the cause of the case 'emerging' in the first place. Therefore, it is reasonable to distinguish between the statistical generalization and analytical generalization. Statistical generalization aims to extrapolate the identified causes in a sample to the entire population whereas analytical generalization strives to theorizing based on the case. In the current case study, we lean towards analytical generalization in the sense of explaining "how" and "why" the phenomenon of eID public acceptance occurs, what are its causes and what implications it bears. Indeed, the nature of the case calls for a specific question of whether it can be replicated in other contexts, i.e., other countries, but one must accept that all observations and findings are the cause of a particular and unique context. Hence, a more appropriate task is to provide explanations on an abstract and theoretical level that can then be transferred to a different context. To ensure such transferability is possible, Yin's hints on addressing the issue of external validity during the research design phase and making sure the case study uses the right theories and/or theoretical propositions. In terms of the current case study research, the research design, and, specifically, the research questions, are carefully considered and backed with chosen theoretical concepts. The received outcomes are then triangulated to increase their validity.

Reliability refers to demonstrating that the operations of a study - such as its data collection procedures - can be repeated, with the same results. The common way to address reliability is to produce a case study report which entirely explains how the case study research was conducted. The current dissertation can serve as the case study report and used to test the reliability of this case study. The chain of evidence has been maintained and documented. The data collected within the entire case study is retained and stored.

3 Theoretical Background

This chapter provides an overview of theoretical concepts that together form a theoretical framework through which this dissertation is viewed and on which it is built upon. The chapter is divided in three subsections where each theory or concept is respectively described. The content of the work within the chapter does not provide an immediate context to the dissertation's subject but does draw general linkages to the field for the better understanding of the text by the reader. The main concepts discussed are the Technology Acceptance theories, Institutional Design, and Actor Network Theory.

Why these theories are important in the context of eID public acceptance? The technology acceptance theories will help the reader grasping the main variables that acceptance consists of, regardless of a kind of a technology we are dealing with. Moreover, these theories are the primary origins of modern concepts of our vision and common knowledge about how and why an invention, a technology, an artifact can be used, is going to be used and why. Further, in Section 5.2 we will see that the factor of eID public acceptance are emanating from technology acceptance theories but in a more specific form. As for the Institutional Design framework and Actor Network Theories, these will navigate the reader through the relations of stakeholders on different institutional levels and in different settings. The two theories complement each other and help interpreting the complex interactions among the participants of the Estonian eID ecosystem, including end-users themselves.

3.1 Technology Acceptance

One of the priorities of decision makers has been to identify the factors that influence users' intention to use a particular system. This knowledge can be taken into account during the development phase. The question of why and how new technologies are accepted by people has been on the radar of both researchers and practitioners [114].

Over several past decades, a series of theories, concepts, and frameworks have been designed to explain the user adoption of technologies and variables that affect it. Among those are the Technology Acceptance Model (TAM), Theory of Planned Behaviour (TPB), Theory of Reasoned Action (TRA), Diffusion of Innovation theory (DOI), Unified Theory of Use and Acceptance of Technology (UTAUT) and many other theories and models that derived, been extended or modified by means of various constructs. For instance, [114] who reviewed the technology adoption models and theories, also includes a model of PC Utilization, a social cognitive theory, and a motivation model (see Figure 2).

Given a wide array of models that explain the adoption of technologies, over the course of the research within this dissertation, the constructs of the following models and theories were used and applied in regards to factors of eID public acceptance: Theory of Planned Behaviour [11], TAM [45], UTAUT [130]. These models and theories and their extensions are discussed below in the further subsubsections.

3.1.1 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) that was introduced by Ajzen in [11] is a contemporary version of the Theory of Reasoned Action (TRA) from Fishbein and Ajzen [49]. TRA is composed of three cognitive components, i.e., attitudes (unfavourableness or favourableness of person's feeling for a behaviour), social norms (social influence), and intentions (individual's decision to behave in a certain way). The foundation of TPB is built upon three independent predictors of intention: attitude toward behaviour which stands for "the degree to which a person has a favourable or unfavourable evaluation or appraisal of

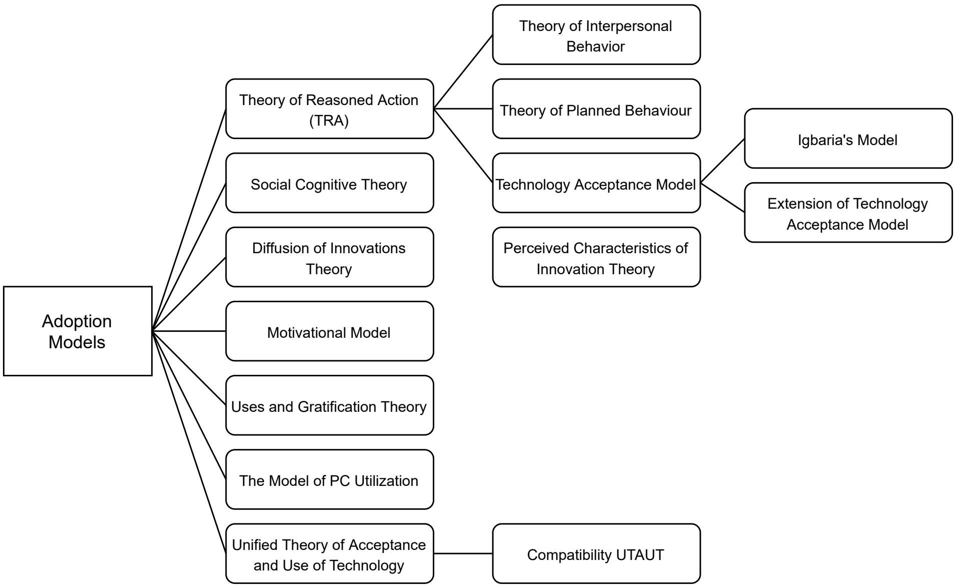

Adoption Models
Theory of Reasoned Action (TRA)
Social Cognitive Theory
Diffusion of Innovations Theory
Motivational Model
Uses and Gratification Theory
The Model of PC Utilization
Unified Theory of Acceptance and Use of Technology
Theory of Interpersonal Behavior
Theory of Planned Behaviour
Technology Acceptance Model
Perceived Characteristics of Innovation Theory
Compatibility UTAUT
Igbaria's Model
Extension of Technology Acceptance Model

Figure 2: Adoption models overview by Taherdoost [114].

the behaviour in question" [11]. The second determinant is subjective norm, a social factor that refers to "the perceived social pressure to perform or not to perform the behavior" [11]. The third construct is the perceived behavioural control which means "perceived ease or difficulty of performing the behaviour and it is assumed to reflect past experience as well as anticipated impediments and obstacles" [11].

As Taherdoost notes [114], the third variable in TPB poses realistic limitations on the individual's actions which are not always under volitional control. In TRA, the crucial condition is that person's actions are systematic, rational and, most importantly, voluntary. This creates an issue with validation of TRA. However, TPB has also received its criticism which is the exclusion of emotions and habits as influencing factors. Additionally, some researchers point out the extent to which certain beliefs can as mediators affect the outcome of IT adoption and its use. As Jokonya notes [58] the perceptual beliefs can be difficult to understand in terms of the degree of their possible influence. Moreover, another weakness of TPB is the "lack of explanatory power of testing different IS contexts since its original constructs do not fully reflect every context" [58].

3.1.2 Technology Acceptance Model

Technology Acceptance Model (TAM) by Davis [45] is perhaps the most influential theory on the adoption of technology in IS research [24, 58, 97, 114]. TAM by Davis and its family of approaches are discussed in this subsection and referred to as simply "TAM".

TAM derives from the TRA [45]. While TRA is a theory that explains human behaviour, TAM was designed to model user acceptance in the IS domain [39]. Originally, the intention was to apply the model specifically to construct the users' acceptance within an organization where information systems (e.g. emails and computers) are introduced to increase productivity and quality of work, optimise job-related processes [45].

TAM consists of two dimensions: Perceived Usefulness (PU) and Perceived Ease of Use (PEU). Perceived Usefulness in an organizational context refers to "the degree to which a person believes that using a particular system would enhance his or her job performance"

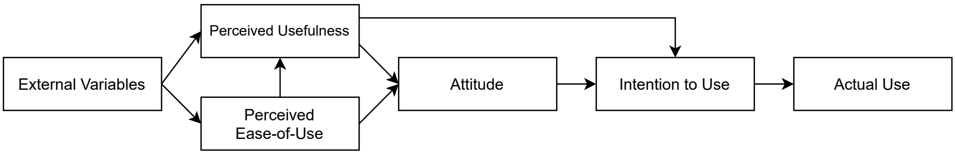


Figure 3: Technology Acceptance Model by Davis [45]

and Perceived Ease of Use refers to "the degree to which a person believes that using a particular system would be free of effort" [45].

As Figure 3 shows, the user acceptance presents itself as a four-stage process during which the decision to use the technology transforms under the impact of particular variables.

TAM originally aimed to study acceptance and system use by employees in an organization [45]. After theoretical analysis and synthesis of various theories such as self-efficacy theory, human-computer interaction, diffusion of innovations, marketing, expectancy theory and others on the subject of perceived ease of use and perceived usefulness, validation of the model was conducted after carrying out several field and lab studies where users were testing software (e.g. a mail system, a file editor, a graphics editor). An outcome was that the correlation of both constructs as determinants of acceptance were significant. Especially, this concerned the perceived usefulness. As Davis explained, the primary motivation for the user to adopt a systems is the function it performs and the value it brings as a consequence of its use, and only after that secondly comes the ease of its use. He further mentions that users are quite often ready to cope with some difficulties during the use of system if the function it performs is critically important for them. This surely may discourage the adoption of a system to a certain extent, however, if this system does not deliver a desired outcome, any amount of ease of use can be otherwise disregarded. This contains an important message to designers and developers who are strongly suggested to consider usefulness and its human factor dimension as an element of a successful system [45].

However, TAM has received its portion of criticism. Efforts have been made to address TAM and its further extensions' lack of guidance. One of the best known models were introduced by Venkatesh and Davis [128], where first criticism on TAM was discussed. As the authors state, TAM " [...] is predictive but does not really offer enough to help designers and managers to alter the course of the fate of a system because it simply states that the more the usefulness and the more the ease of use, the greater the use."

Later, this gap was attempted to be bridged with TAM's extensions and derivatives. Mainly, same researchers, Venkatesh and Davis, presented TAM2 [129] where the focus was put on identifying the determinants of one of the predictors: perceived ease of use (see Figure 4).

Following the TAM2, Venkatesh then introduced another set of determinants for the perceived ease of use. These include anchors (i.e., computer self-efficacy, perception of external control, computer anxiety, and computer playful-ness) and adjustments (i.e., perceived enjoyment and objective usability). Venkatesh informally, as he puts it himself, refers to this model as TAM2' in order "to reflect its complementary role to paper on the determinants of perceived usefulness." [126]

As a result of theoretical synthesis and integration with an empirical set, Unified Theory of Acceptance and Use of Technology was designed. It will be described in detail further below. To conclude with the TAM evolution and its extensions, in 2008, TAM3 was introduced by [127] as a result of endeavour to study interventions by introducing

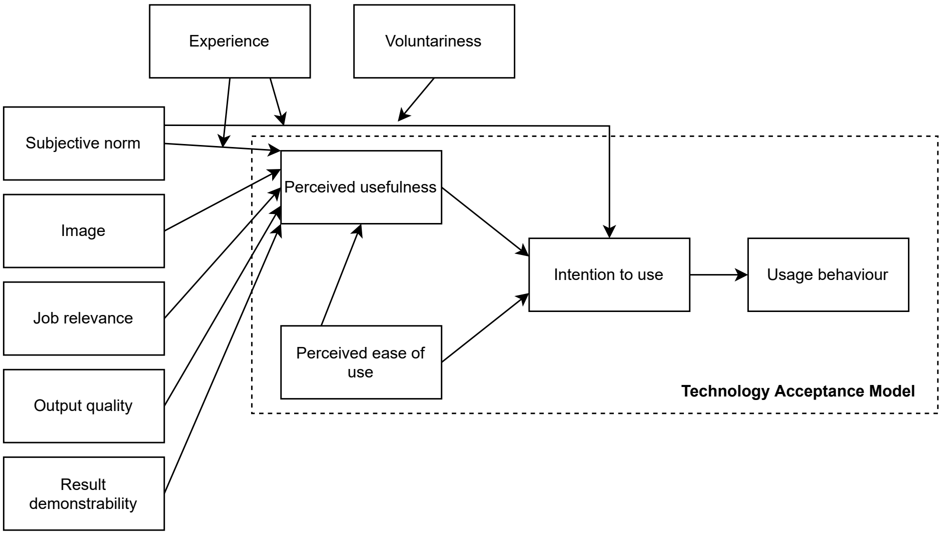


Figure 4: Determinants of Perceived Usefulness in TAM2 by Venkatesh and Davis [129].

enhancements for promoting employees' acceptance [126]. Ultimately, in TAM3 its predecessors TAM2 and TAM2' are merged

3.1.3 Unified Theory of Acceptance and Use of Technology

Inspired by TAM, UTAUT model was introduced in 2003. Aiming to address TAM's lack of guidance, a new theory was designed as a result of synthesizing thirty two constructs across eight models with an outcome of four variables significant in their conjunction to the analysed models [130].

Four significant predictors, introduced by Venkatesh are performance expectancy, effort expectancy, social influence, and facilitating conditions. They are defined as follows. Performance expectancy refers to "the degree to which an individual believes that using the system will help him or her to attain gains in job performance" [130]. Effort expectancy is defined as "the degree of ease associated with the use of the system" [130]. Social influence is "the degree to which an individual perceives that important others believe he or she should use the new system" [130]. Facilitating conditions are defined as "the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" [130]. Together with the four core predictors, four moderating variables are added: age, gender, experience, and voluntariness of use (See Figure 5).

When it comes to criticism of UTAUT, the author of the model indicates the following in his paper where he reflects on the developments ten years later since the moment the model has seen the world: "...although UTAUT offers more precise prediction of technology acceptance given the greater amount of variance explained and the various contingencies in the model, like TAM, it is lacking in terms of providing design or managerial guidance."

Still, a meta-analysis of the UTAUT model by Dwivedi et al. [48] suggests its strong validity, noting a high or mixed significance of the relationships between the model's predictors and external variables . The study also revealed the trend of introducing a growing number of different external variables when it comes to the evaluation of acceptance. The author of UTAUT himself introduced in 2008 yet a further modification of the model, the UTAUT2, as the consequence of the technology expansion beyond the workplace context.

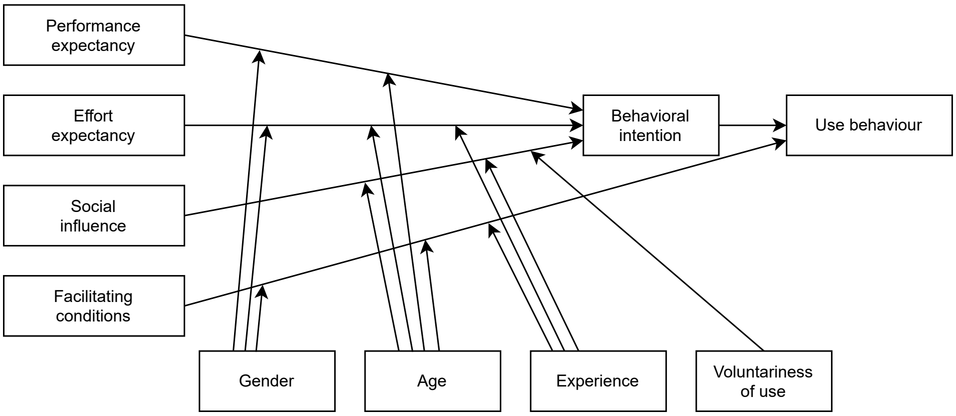


Figure 5: UTAUT.

The updated model considers "specific contexts can bring about changes to existing theories in various ways." [126] The new additional variables are hedonic motivation, price value, and habit. The hedonic motivation refers to "the fun or pleasure derived from using a technology" [131]. The price value is defined as "consumers' cognitive trade-off between the perceived benefits of the applications and the monetary cost for using them" [131]. The variable of habit is defined as "the extent to which people tend to perform behaviours automatically because of learning" the extent to which people tend to perform behaviours automatically because of learning [131]. Among other updates in UTAUT 2, the moderating variable of voluntariness of use is dropped since the model itself targets the consumers' context where unlike in the workplace setting, the use of system or solution is fully voluntary and hence is redundant. In this sense, for the case of Estonian eID, the UTAUT2 was obviously dismissed as it does not fulfil two criteria: 1) the voluntariness of use (as eID in Estonia is mandatory to have); nor 2) the context is not consumer-related since in the case of Estonia, the nature of relationships between the user of the system/solution can be qualified rather in terms of e-government, i.e., G2C (government-to-customer), G2B (government-to-business), or G2G (government-to-government).

If we come back to the first and original version of UTAUT [130] and couple it with the context of public acceptance of eID, UTAUT is not sufficient be solely applied for the eID adoption case of Estonia. It is worth to repeat the weakness of this model and note that some contexts may require different changes in the models' constructs. This also underpins the relevance of this dissertation due to the need of identifying external variables which might have a significant impact on the public acceptance. Furthermore, even if we zoom out to the context of e-governance and the respective applications of technology adoption models within such scope, the use of single model will not provide a full overview and explanation of the public acceptance. Be it TAM or UTAUT, one variable or another will remain uncovered and will require external determinants to be introduced in the equation. Only one or two decades ago, a system was far more primitive than nowadays, consisting of a PC with a standard software with a single user/employee in an organizational setting [39, 10]. However, today and further in the future, IT systems are and will be designed using a different logic offering a range of personalized and context-based e-services [39].

3.2 Institutional Design by Koppenjan and Groenewegen

It is not enough to discuss the phenomenon of public acceptance purely by dissecting it into constructs and looking into the relationships between them. These constructs exist in an environment that is far away from being isolated from external influences. It takes much more to track and identify all of these than just simply tweaking the known determinants in order to find the right ratio and reach acceptance.

Public acceptance is both an outcome and an instrument. An immense amount of time, efforts, resources, and conditions are standing behind public acceptance as an outcome. Therefore, in this subchapter, the perspective of institutions will be discussed. The aim is to unveil the potential of institutional design when it comes to large-scale information systems such as e-governance, e-government, and eID.

In [64], Koppenjan and Groenwegen present an analysis framework (see Figure 6) aimed for a certain range of large-scale technological systems that "do not consist merely out of technological assets, but involve institutions as part of their solutions" [27]. The complexity of such socio-technical systems is explained by numerous dependencies that exist between their institutional and technology parts. According to KG, these complex technological systems consist of technology component which is important however does not merely determine the functioning of the entire system. What matters also is the behaviour of actors (individuals, groups or organizations) who actually make the decisions on the system, its development and functioning.

Another aspect is that these systems are characterized by multiple actors involved. Very often, they consist of more than one organization but rather of a constellation of organizations. Next, the actors and institutions of such complex technological systems include both public and private parties which are impacted by the functioning of the system. Lastly, the latter is influenced by such forces as government regulations (on multiple levels) and market forces (demand, competition, cost).

Koppenjan and Groenewegen state that the way these systems are designed in turn determines the coordination of actors' behaviour that allows the system to function. The coordination is facilitated by "institutional arrangements that regulate the positions and relations between parties" [64]. Hence, apart from the substantive and technological designs necessary to design the systems, institutional design is required as well. While Koppenjan and Groenewegen [64] couple technological and institutional designs, they outline the third kind of design – the process design. Considering the complexity and number of actors involved, systems are adapted during the "processes by which they were agreed upon and implemented". This means that design is not created once and is then set in stone. It is rather an iterative process that is stretched in time and requires interaction of parties resulting in agreements and incremental steps. It aims to improve and structure this process. Hence, as Koppenjan and Groenewegen put it, "process design is thus concerned with designing the design process" [64]. This pre-supposes who should be involved, how this involvement should take place, what rules and regulations determine this process, what conditions and requirements should be met and who is in charge of it.

Complex technological systems involve many actors and in order for the system to function, coordination is required. By themselves, technological systems cannot operate. They must be driven by a set of rules, or, as Williamson argues, "rules of the game" [136], that will guide the behaviour of actors. These rules can be framed as formal or informal laws that can have a private or public character. [64] regard these rules as institutions which are required for the system to function. Yet, not all arrangements, rules, or agreements can be considered as institutions or institutional arrangements. In their works, Goodin [51], Bush and Tool [37] agree that these arrangements must be commonly ac-

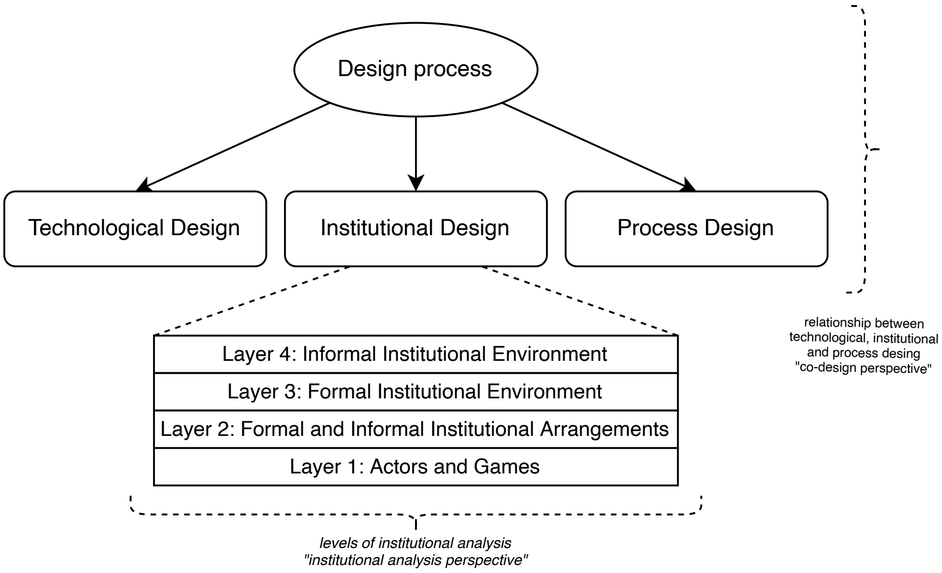

Design process
Technological Design
Institutional Design
Process Design
Layer 4: Informal Institutional Environment
Layer 3: Formal Institutional Environment
Layer 2: Formal and Informal Institutional Arrangements
Layer 1: Actors and Games
relationship between technological, institutional and process desing "co-design perspective"
levels of institutional analysis "institutional analysis perspective"

Figure 6: Institutional design model by Koppenjan and Groenewegen [64]; adapted from [27].

knowledged by the involved actors, they must be utilised in practice and must be valid for a certain amount of time.

Koppenjan and Groenewegen [64] warn about the problem of collective action and a high degree of likelihood it is going to occur. They define this problem as such that arises due to the multiple actors' interests and their occasional collision. Once the conflict occurs, the situation requires a solution which is impossible without parties cooperating with each other. Because of the parties having different motives and reasons to participate, there are significant costs and risks coupled with the decision to join. The costs can be related, for example, to the compromises that actors have to accept, or to efforts to interact with each other. The risks can be associated with the dependency on each other and the possibilities that one's interests may face negative implications of others' strategic or opportunistic behaviour [64]. In other words, the interaction between the involved parties is both a key to make the technological systems to function and a source of costs and risks coming from the participants themselves. Therefore, the need for the institutions and institutional arrangements is justified and has to be fulfilled.

Going further, Koppenjan and Groenewegen[64] specify the institutions by using four levels of analysis by introducing and adapting the model of Oliver Williamson [136, 137]. The adaptation of the transaction cost economics model is twofold: firstly, a layer of the actors and their strategy is added; and secondly, Koppenjan and Groenewegen [64] enable the interaction between the four layers of the model (see Figure 7).

Layer 4 that refers to "culture, values, norms, attitudes" which are the informal "rules of the game" that significantly impact the mindsets of actors in networks from Layer 1. It also influences the actors' perceptions of what is considered to be a problem, how is it identified, and what kind of a solution is seen as feasible.

Layer 3 represents the legal and formal rules of the game. They determine the legal positions of actors and the legal mechanisms that regulate the transactions.

Layer 2 contains actors who join into networks in order to design rules and mechanisms that coordinate the transactions among them. For example, "governmental structures"

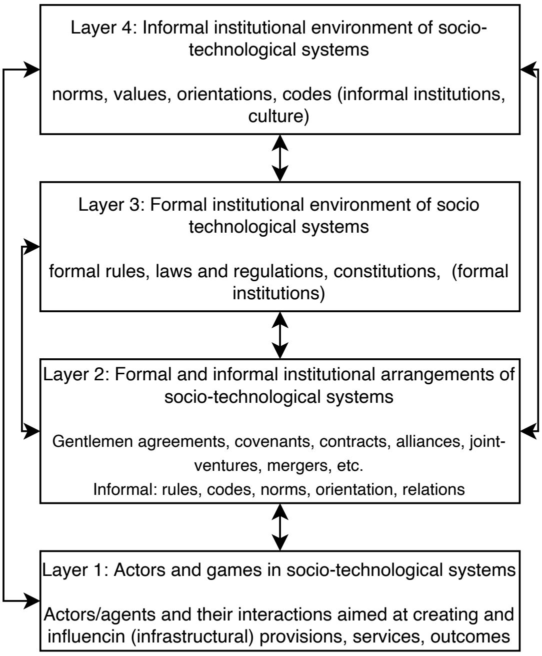

Layer 4: Informal institutional environment of socio-technological systems
norms, values, orientations, codes (informal institutions, culture)
Layer 3: Formal institutional environment of socio technological systems
formal rules, laws and regulations, constitutions, (formal institutions)
Layer 2: Formal and informal institutional arrangements of socio-technological systems
Gentlemen agreements, covenants, contracts, alliances, joint-ventures, mergers, etc.
Informal: rules, codes, norms, orientation, relations
Layer 1: Actors and games in socio-technological systems
Actors/agents and their interactions aimed at creating and influencin (infrastructural) provisions, services, outcomes

Figure 7: The four-layer model: levels of institutional analysis [64] adapted from Oliver Williamson [136, 137].

can be defined as institutional arrangements that regulate a specific group of transactions among several agents concerning a certain asset. On this level, the agent also form associations, networks, and public-private partnerships or arrangements.

Layer 1 consists of individual agents and their interactions for the purpose of generating "(infrastructural) provisions, services, and outcomes" [27]. Koppenjan and Groenewegen address large-scale systems such as "energy networks, water management services [. . .], waste treatment, transport systems (rail, road, water, tube), industrial networks, information systems and telecommunication networks, city service [. . .]" [64]. Even though, the information systems are included in the range, as Bharosa et al. point out [27], the model itself becomes relevant in case that an information system goes beyond the scope of a regular enterprise architecture but rather can be defined as a ultra-large-scale software system [89]. Therefore, Bharosa, et al. conclude that [27], in the context of e-government systems, the model is highly relevant and can be used for theoretical analysis. Within this dissertation, the eID will be analysed and discussed through the prism of the Koppenjan and Groenewegen's institutional framework.

3.3 Actor-Network Theory

Actor-Network Theory (ANT) is a theory from the field of social studies of sciences and technologies created by Bruno Latour, Michel Callon and John Law. The main difference that distinguishes this theory among others is its rejection of the "social" element together with the concept of "social network" whatsoever. Latour asserts that networks consist both from human and non-human entities which are equally important to the network.

Within the ANT, the (non-)human actors of the networks are also referred to as the actants. According to authors, each actor, depending on its role, purpose or relation to other actors, can take any shape [68]. That is where another central idea of the ANT lies, which assumes that no one and nothing is beyond the network of relations. Each actor has no difference in its abilities, be it a person, an animal or an inanimate object. Nearly any actor can be split into smaller actors, which implies that an actor can be a network consisting of other actors. In her review of "Reassembling the Social: An Introduction to Actor-Network-Theory", Wessells identifies Latour's main premise of the theory as "an amalgamation of social entities" [135]. She then defines the amalgamation in the context of governmental structure such as "city government" which "is a tangled, temporal knot of agencies, personalities, connotations, services, buildings, phone systems, offices, elected officials, meetings, websites, vehicles, programs, uniforms, press releases, department heads [. . .]" [135]. The claim is that we are aware of it as well as of the fact of how these components interact with one another in ways that what we mean and call a "city government". But the problem here, according to the criticism of Wessells, is that we often fail to grasp adequately how in fact these components do interact, and as a consequence, we turn the "city government" into something much more stable than it can be. From here, another distinguishing aspect of the theory arises which is also linked to the fact that the ANT is not always seen as a "theory" but a "method". More precisely, the ANT is material-semiotic method that aims to examine thoroughly the relationships between the elements of the network. The ANT attempts to explain how material-semiotic networks form into a whole to act the way they do. Now, the "material" and "semiotic" qualities mean that these networks are simultaneously mapping relational ties between things (material) and concepts "semiotic". One of the things that we tend to do is looking at strategies and patterns that join the different elements into clusters of actors and networks so they become an apparent whole. These networks are likely to be transient, impermanent, and subject to constant assembling and re-assembling. It then follows, that in order to maintain a network and keep it from "dissolving", it is necessary to "perform" these relations continuously [68].

The networks are also featured as not intrinsically coherent which means there can be conflicts and contradictions. It also follows that (social) relations only stay in process and have to be maintained or "performed".

Wessells summarizes this concept in her review, again, from the perspective of a governmental project on building a new waterfront that she uses as a scenery for the ANT. "The notion that there is one agreed-upon, well-operationalized vision for a new waterfront open space that is then implemented and achieved is not borne out by field research. Instead, I have found that these projects are best understood as continual works-in-progress, evolving over the course of decades and through the differing, adaptive efforts of multiple participants." [135]. What she is attempts to explain, is that there is no blueprint on how to execute a project or a policy by simply studying a case once in field conditions and after replicating all the steps next time. Because of the involvement of so many actors and their clusters, it is very unlikely that the same scenario will repeat itself. Here, Koppenjan and Groenewegen's institutional design can complement the premise of Latour by one of its constructs discussed in the preview subsection. More particularly, when referring to the problem of collective action [68], it becomes apparent that interests of so many parties involved create conditions that determine the course of interactions and relationships between the actors. Moreover, these relationships need to be maintained (or performed) through a series of agreements, negotiations, and compromises.

The parallel that Wessells draws [135] with the government project she describes in her review of Latour's book, indeed provides a clearer understanding of the theory that is applied in a more tangible scenario. It must be noted here that Wessells, yet, calls for [135] not applying the theory in practice but rather to rely on its tenets. As she writes in the review “Researchers should take their time, tracing mundane interactions between connected sites and actors. Collecting records of these interactions allows us to see how sites and actors mediate between one another, at the most basic levels of connection.” [135]. Again, it is difficult not to refer to Koppenjan, J. and Groenewegen [64] again and the institutional levels they adapted from Williamson [136, 137]. Although Wessells is appealing [135] to researchers about the method with which to apply the ANT, in fact, the subject of this appeals, i.e., the interactions between the actors, resembles the formal and informal institutional arrangements (Level 4 and Level 2; see Figure 7).

Within this dissertation, both the institutional design framework and the ANT will be applied in the context of eID and its public acceptance in order to conceptualize this phenomenon and depict the connections of theoretical constructs with a real-life case. The aforementioned will appear later in Chapter 6.

4 Case Context Description: the Estonian eID

The description of Estonian eID and its ecosystem is provided in frames of the case study methodology by Yin [139]. This case context description is intended to give a sufficient background information that will help to understand and follow the case at hand.

4.1 ID card and electronic identity setup in Estonia

Estonian ID card is a mandatory identity document for the citizens who are aged 15 and over. It is used for physical identification but can also be used as a travel document by citizens that travel within European Union [2].

The ID card contains a chip which enables the card to be used digitally as it is based on public key infrastructure (PKI). PKI allows for a secure authentication and legally binding digital signing. The first ID cards were issued in 2002. (e-Estonia) It allowed to replace the first passports that were issued back in 1992 and were about to expire after 10-year validity [76].

The concept for a new type of ID which is essential an electronic identity document appeared between 1994 and 1995 in the Institute of Cybernetics (Taltech) [92]. As the CEO of the Estonian Certification Authority (CA) recalls during the interview conducted in the third round of research within this dissertation, the experts from Cybernetica AS were specializing on cryptography and "were able to provide… baseline cybersecurity knowledge".

It was realized later in 1997, as the former Citizenship and Migration Board (now Police and Border Guard Board) started to discuss the need of introducing such a document [92]. However, the discussions and decision-making took more time than expected, so that planned 15-month deployment was stretched to almost four years. *(Ibid.)*

Aside from that, there was also the process of establishment which was complex in general and required preparing respective legislation which was the Digital Signatures Act. It was passed in 2000. This created a need to establish a certification authority. It was founded in 2002 by the two biggest banks and telecom operators. The certification authority handles the public key infrastructure of Estonian eID and is a private-owned company SK ID Solutions AS, previously known as AS Sertifitseerimiskeskus (SK) [76].

The function of the certificate is to provide a binding relationship between the public key and the identity of the cardholder. The authentication key is used to log into the e-service environment. The same key can be used for the decryption of a document that was encrypted for the cardholder. PIN1 is used for these operations. The digital signature key is used to provide a legally binding digital signature. Under the eIDAS Regulation, it is recognized as a qualified electronic signature. PIN2 is used for this operation [95].

Aside from authentication and digital signing, the ID card has another functionality in a form of the personal data file that is contained in the chip. The file contains 16 records of information which is printed on the card. The ID card issuance is a public service provided by the Estonian state [76].

Beside the ID card, there are several other types of electronic identity proof.

Digital ID card or digital identity card is a digital document that can be used for authentication and digital signing purposes in an electronic environment. Digital ID card cannot be used to identify the person. Citizens or residents who hold a mandatory ID card can apply for a digital ID card which upon issuance will be valid for 5 years [2].

e-Resident's digital ID is issued to an alien by the Estonian state based on the identity of a nationality the person holds. It is a digital document that can be used to identify the person and provide a digital signature only in an electronic environment. The holder of e-Resident's digital ID can perform electronic transactions and benefit from e-services provided by the Estonian state regardless of his physical location [3].

Mobile ID was introduced in 2007 by the largest telecommunication provider EMT in cooperation with the Estonian Certification Authority. (Martens 2010) To obtain a Mobile ID, the user has to replace his regular SIM card with PKI capable one. Then the Mobile ID needs to be "activated" through ID card after the mobile operator registers the user. The certificates contained in the SIM card hold the same personal information the ID card does.

One of the advantages Mobile ID has is that the user does not need to have the ID card and a card reader with him and can use his phone instead. Especially, this is relevant for the share of users who do not own smartphone but continue to use regular cell phones.

Smart ID was launched in 2017 by the SK ID Solutions AS, the state's Certification Authority. It was developed in cooperation with Cybernetica. Smart ID utilizes a smart device as a tool for authentication and digital signing. Smart ID operates on the basis of proven cryptography principles via PKI. The advantage of Smart ID over Mobile ID is that it does not require a SIM card either. The initial goal for the solution to achieve was to help banks overcome the restrictions imposed by the security regulations back in 2016. However, the app quickly became popular as a convenient authentication tool and outreached its initial goal [88]. In 2018, Smart ID became recognized by EU as a Qualified Signature Creation Device that users can use to sign documents digitally with Qualified Electronic Signature according to the eIDAS regulation. [20] In 2019, Smart ID was announced to be used as an authentication tool to the state e-services. *(Ibid.)* Smart ID is considered a successful solution that rapidly engaged new users immediately after launch. The SK ID Solutions started to provide the service also for Latvia and Lithuania. Within a year and a half, the solution gained more than a million users [88].

4.1.1 Other Authentication Methods

Banks started to introduce online banking services in 1996 [95]. PIN-calculators and password cards were used to authenticate bank clients. A PIN calculator is an offline card reader with a key pad that the user used upon log in to his online banking. The user would receive a code number on the screen, after which inserted the bank card to the card reader and entered the number received on the computer screen. The PIN calculator would then generate a one-time PIN that the user inserted online. A password card issued to a bank customer was another authentication method. It contained 24 different codes one of which the customer would insert upon logging into the online banking [76].

Later, in 2000s, as a federated authentication service, banks started to provided so-called bank links for the third parties [95]. Many governmental authorities also implemented this service since banks were considered trustworthy. Nowadays, the PIN calculators and password cards are being phased out not only particularly for governmental services, but overall due to weak security of the given authentication method [92].

However, even after the launch of ID card and Mobile ID, bank-provided authentication methods remained widely popular. For example, the statistics on the use of authentication means used to log into state governmental portal, a one-stop-shop for accessing e-services, shows that up until 2014, among other eIDs, bank links prevailed, after which to diminish. At the same time, Mobile ID started to be used more consistently. *(Ibid)*

4.2 Stakeholders

The lifecycle of an ID cards is maintained by a significant list of parties each of which has clear and vital functions and responsibilities. The history of relations among the stakeholders is beyond of this work's scope and only few and key events presented in this chapter with the aim to provide sufficient background information.

The ID card starts its journey at the manufacturers' facilities. Firstly, the smart card manufacturer is responsible for producing the smart card chip microcontroller and the operating system for it. Secondly, the manufacturer of ID card embeds the chip into the plastic card on which the cardholder's information is printed, and then personalizes the chip by recording electronic information into it [95]. At this stage, the public-key certificates provided by the Certification Authority are loaded into the chip. The ID card is then ready to be issued to the card holder. This role is performed by a government authority that is responsible for issuing the document to a verified person. Today, the government authority to perform this duty is the Police and Border Guard Board (PBGB), but until 2010, it was the Citizenship and Migration Board that was eventually merged with several other authorities. PBGB issues ID cards, ePassports (machine readable travel documents), and temporary residence permit cards [95]. PBGB is supervised by the Ministry of Interior, while the Ministry of Economic Affairs and Communication is supervising the State Information Systems Authority which in turn coordinates ICT in the public sector [76]

Besides the parties mentioned above, banks are also involved into the eID constellation of actors since they operate as Registration Authorities. For example, today, a person with an valid ID card can use bank's assistance to get registered as a Smart-ID user.

4.3 eID Diffusion and Promotion

After the first ID cards were issued, they were not popular among the citizens, and in fact, nobody could understand or did not know how can it be useful. However, the situation started to change in the first years as efforts began to be invested in the diffusion and promotion of the new eID [76]. While the public sector, particularly, the Ministry of Economic Affairs and Communication, was working on the diffusion of ID cards alone, the certification authority, i.e., SK (now SK ID Solutions) had to make sure the software and smart card readers for ID cards were distributed as well. The motivation to do so was strong as SK's existence on the market depended on whether the eID cards were used or not. Hence, strong commitment on the side of the private sector from the beginning of the ID card launch was crucial for its success. *(Ibid.)*

Having prioritized the direction towards the IT, in 2001, several the most impactful companies around Estonia established a foundation Look@World, main goal of which was to promote Internet to Estonians. As a result, a great deal of resources has been spent on teaching people how to use the new technology. Multiple channels have been included to deliver to the public the knowledge about the new solutions and create motivation to use them. Focused joint efforts have been put into spread of knowledge about the technology to increase population's computer literacy.

In 2006, the members of the Look@World foundation, i.e., Seb Bank, Swedbank, telecom providers Elion and EMT on the private sector side together with Ministry of Economic Affairs and Communication on the public sector signed a cooperation agreement called "Computer Security 2009" with an ambitious mission to form Estonia as the most secure computer and information society. Many other e-service providers joined the project [90]. The beneficiaries were the Internet and e-service users. A wide usage of the ID card and Mobile ID usage was promoted. During the fund allocation for the planned projects, it was realized that while the importance of IT was growing day by day, the analysis showed that nearly 300,000 citizens were not using computers and Internet due to the lack of skills, motivation, and financial resources. Hence, the Look@World foundation and a few other private companies launched a project "Come along!" with an objective to provide basic and advanced computer training to 100,000 people and provide Internet access to 50,000 families. Free trainings and affordable prices on Internet access and computers were offered [90].

The scope of the “Come along!” project was training courses on the ID card, Mobile ID, and e-services. Particular attention was paid to beginner level users. The premise of the project strategy was that low motivation to start using computers and internet stemmed from the lack of knowledge how to do so.

A training project “eCitizen’s Training Network” was launched in order to spread knowledge on ID card, Mobile ID, and e-services and was held in a classroom format with teachers who received special training. In total, around 30,000 people have received training on e-services use, basic and advance computer and Internet use skills [90].

An important part of this initiative was to ensure an even spread of training. To reach remote locations, an eBus project was launched, where the educating process would take place in a format of “classroom on wheels”. During this project, around 195 trainings were arranged with 1,200 people. As an encouragement, it was possible to receive card readers free of charge.

Among other initiatives were the mobile training boxes located in busy and crowded places that offered practical personal training on ID. As a result, it yielded over 14,000 people receiving the training, and more than 20,000 getting assistance from the boxes. There were also established eService’s consultation centers that provided personal advice on the e-services usage. Additionally, an ID support center was opened to provide assistance delivered through several channels: ID website, ID support website, a phone hotline and an email address [90].

Last but not least, a mentoring programme to the “Come along!” project was launched in 2009 with the aim to help people by providing extended computer trainings and overall IT assistance by involving volunteers and forming communities [90].

4.4 ID Card Application

The ID card has a wide range of use cases it can be applied in. Apart from a long list online services, ID card can be used for the next purposes.

e-Ticketing. Citizens are able to purchase online tickets to use public transportation. By personalizing their ticket with their ID card, citizens can claim the fare discounts the are entitled to. For instance, residents of Talinn and Harju county surroundings can use public transportation for free once they link their e-ticket to their ID card [76, 5].

e-Voting. Estonia is the first country to run internet voting on a national scale. Using an ID card or a Mobile ID, it is possible to submit a vote from whatever location in a secure and convenient way [IX]. Nowadays, more than 40% of voters prefer the online method.

e-Prescription. By means of a centralized paperless system, doctors are able to issue and handle medical prescriptions. A form is filled electronically by the doctor, and once the patient presents his ID card in the pharmacy, the pharmacist is able to see the record in the system [4]. An ID card holder can also check online his health records.

Additionally, an ID card is a partial replacement of a driver’s license. Drivers do not need to carry their driver’s license with them, since upon the need to present it, they can hand in their their ID card instead [76].

5 Results

This chapter reports on the results of analysis of four data collection rounds. Each section of this chapter represents one of the three units of analysis within this case study. Section 5.1 presents the description of the background of this dissertation reporting on how the study commenced in the first place with the emergence of the public acceptance subject as the main focus of our work. Section 5.2 reports on the results of the SLR and presents the factors of eID public acceptance. Section 5.3 elaborates on the citizens perceptions of and attitudes towards eID in Estonia. Section 5.4 reports on the results of thematic analysis of in-depth experts interviews about eID, its public acceptance and overall importance in the context of a successful e-government. The research methods and data collection procedures are described in detail in Chapter 2.

5.1 Initial Findings on the Subject of Public Acceptance

As it was mentioned in Chapter 2, this dissertation unfolded gradually. Prior to deciding on conducting a case study of Estonia, the subject of public acceptance was discovered during the research about Ukrainian eID (see [I]). Ukraine launched its first electronic identity documents in 2016. Considering the economic and political situation in the country amidst which the government had started its path towards electronic government, this setting presented itself as an interesting and worth investigating research problem. Precisely, the aim of this research [I] (and first data collection round) was to identify key success factors of national electronic identity management systems. At the time of designing this research, related work and theoretical background were studied, in 2017, we revealed grey areas around the research inquiry on user perspective aspects related to national eID management systems. We also reviewed the experience of other countries that are more realized as e-states with more matured eID systems. Estonia was amongst them.

Therefore, keeping in mind all of the above, we designed a questionnaire for citizens attempting to understand their perceptions of, attitudes towards, and awareness about the newly launched eID. That way, not only did we would have a chance to get familiarized with user perspective but also compare and benchmark the development trends in Ukraine to the existing examples. The questionnaire consisted of 14 questions yielded 222 responses. The most significant and eye-catching highlight of the acquired results was the low levels of citizens' awareness and their trust. The thematic analysis of textual responses submitted by citizens showed that among the overwhelming 73% of those respondents who do not trust electronic services, first of all, do not trust the government. Moreover, respondents also replied that they were not aware of the possibility to use the services online. The majority of more than 80% replied that they would like to use public e-services and access them with their eID. More than 60% of respondents also expressed their readiness to provide their biometric data as one of the identity attributes.

Within this research, we additionally conducted a small case study about one of the regional identity solutions that was running in Lviv (also in Kyiv and Dnipro at that time being), one of the biggest cities in the country. The Lviv Citizen Card was launched as a secondary identity document for the residents of the city. It provided a number of benefits online and offline. Apart from being used as a bank card, it also served as a public transportation ticket. The owners could also use the identifier number of the card when applying for a number of online public services (e.g., financial and social aid for certain citizen groups). Our aim was to understand what are the barriers for introducing given solution, and what are the possible future implications for citizens and public service provision from the perspective of local government representatives. Hence, we conducted

3 expert interviews with people who were directly involved in the development, deployment, and service provision process. The interviewees unanimously pointed out to the most significant barrier which was at that time the lack of IT infrastructure and national single identifier. After all, the Lviv Citizen Card is primarily a bank card and is not a PKI-based identity document, so even if the card holder wants to apply for a service online, he or she had to submit an application using a login and password, while the service provider had to make requests to different registries that are not connected to each other. Moreover, often, the applicant still had to submit some of the documents himself by uploading them, sending via email, or presenting them in-person at the local government office. The interviewed experts also predicted that these barriers would cause similar difficulties across the state when it comes to the use of the Ukrainian eID. Furthermore, it would take at least a few years for everyone to acquire card readers.

The interviewed public officials confirmed that public awareness was one of the key important aspects when distributing the launched card solution in Lviv so the local government run a few information campaigns, held press releases, and made a number of public announcements including those in social media platforms. All in all, the experts during the interviews agreed on a long list of multi-level changes Ukraine should go through to make the eID card work and be used.

Today, the Ukrainian eID card continues to be issued as both physical and electronic identity document. The state is actively transforming itself into a digital state. While eID card is not being widely used on its own as it is in Estonia, it found its place in citizens' smartphones in an application"Diya"[1] (meaning in Ukrainian – *action*) which serves not only as a digital passport but as a gateway and a one-stop-shop for a wide range of public e-services.

The research on the Ukrainian eID established for us a research endeavour that we have been following since then. The case of Ukrainian eID drew attention to the importance of the public acceptance when introducing eID. This called for a question on how to introduce eID that way that it will be used. Henceforth, we began to investigate the case of Estonia. Section 5.1 and the first publication [I] is the synthesis of the first data collection round. It is not included as a unit of analysis in our case study design as it does not provide direct findings about the case context of Estonia but it is a foundation of this dissertation and is included as a result of the very first data collection round.

5.2 Factors of eID Public Acceptance

This section reports on the results of the analysis of a second data collection round [III]. The aim of the results is to address RQ1. Table 8 summarizes the outcomes of the conducted systematic literature review (SLR). The main research question within the SLR corresponds to RQ1 of this dissertation: *What are factors affecting eID public acceptance?*

First, we identify a research gap in the existing work on public acceptance that focuses on theoretical aspects derived from technology acceptance theories [15, 16, 52, 60, 103]. Second, search criteria were formulated to address research question RQ1. Third, a literature search was conducted according to SLR guidelines of Kitchenham [63]. After reviewing the search results, 39 items were selected on the basis of having an explicit insight on the citizen perspective of eID and its public acceptance. The selected sources were further thematically analyzed and categorized. We grouped the identified notions, i.e., units corresponding to a factor, aspect, or phenomenon, that were emphasized by the author of the selected source as a valid cause and impact on public acceptance, into twelve categories that are elaborated below.

[1] https://diia.gov.ua/

Table 8: Categories derived from SLR (adapted from [III]).

Complexity	[35, 40, 43, 55, 59, 72, 75, 109, 9]
Ease of use	[7, 8, 12, 15, 19, 43, 52, 55, 59, 72, 13, 87, 92, 98, 104, 108, 109, 9, 115]
Functionality	[19, 40, 43, 116, 52, 55, 59, 62, 72, 13, 87, 92, 104, 109, 50], [I]
Awareness	[7, 12, 17, 19, 38, 40, 116, 55, 59, 69, 13, 79, 87, 92, 104, 109, 50, 9, 115], [I,VI]
Trust	[7, 15, 16, 14, 17, 19, 23, 21, 22, 35, 38, 40, 43, 116, 52, 54, 60, 72, 13, 79, 81, 87, 98, 104, 108, 109, 50, 9, 115, 134], [I,VI]
Privacy concerns	[7, 8, 16, 14, 23, 21, 22, 40, 116, 52, 54, 55, 60, 62, 75, 79, 87, 98, 104, 108, 109, 50, 9, 115, 125, 134], [I]
Security	[8, 16, 14, 23, 21, 22, 38, 40, 116, 54, 59, 60, 71, 87, 108, 109, 50, 9, 115, 134], [VI]
Control and empowerment	[7, 23, 21, 22, 35, 43, 116, 69, 109, 50, 9, 115, 125, 134]
Transparency	[23, 21, 22, 69, 72, 75, 13, 81, 50, 9], [I,VI]
Path dependency	[35, 52, 81, 87, 92, 108], [I,VI]
Cultural and historical factors	[12, 35, 52, 69, 87, 50], [I]

The full outline of the procedures and methods used in this data collection round and analysis are described in Section 2.2.

The descriptions of the categories are taken from [III] as outcomes of the SLR research protocol of Kitchenham et. al [63].

A realm of papers [8, 15, 16, 14, 17, 19, 35, 54, 13, 92, 109, 9] that study technology acceptance, public acceptance, or user acceptance of eID have utilized TAM or one of its extensions [44, 45, 130]. Therefore, the research design of these works is built on the building blocks of TAM and its extentions [8, 15, 16, 14, 17, 35, 109] or these theories are employed as general guidance and direction for the theoretical background. [35, 54, 13, 92, 9]. TAM and UTAUT have also influenced the derivation of notions and factors within this round's analysis as it will be seen further below.

Ease of use. This category echoes the element of TAM that has the same name. This category comprises such notions as "convenience" [8, 35, 40, 43, 60, 92, 50], "user-friendliness" [19, 43, 75, 87, 104], "usability" [8, 19, 43, 55, 62, 9], "comfort" [55]. For instance, Kalvet et al. [60] use the term "convenience" when referring to the physical appearance and properties of an eID card [60]. Such terms as "usability" and "user-friendliness" appear in studies that are having a TAM-oriented view within their methods corresponding with one of the two key variables, i.e., perceived ease of use.

Complexity. This category was distinguished even though it seemingly opposing the "ease of use" almost as an antonym. Here the complexity is seen as an attribute or as a perception. Moreover, among the reviewed literature, this attribute is rather associated with the system standing behind the solution that ends up in the user's hangs. For instance, the system that is seen by one user as "complex" due to the user's lack of awareness or specific knowledge in a certain domain, yet it can still be described so by another user with relevant knowledge, but in the case of the second user, the adjective "complex" has a different meaning [40]. In the work of van Rooy and Bus [125], the term "complexity" is mentioned in the context of information systems and their structure. The issue of complexity in the survey from the study by Harbach et al. [55] can be described as a difficult-to-understand mechanism of the system.

Functionality. This category includes the identified notions that are similar to the "perceived usefulness" variable of TAM. These are the notions "usefulness", availability of options (e.g. authentication methods or e-services available). For example, findings of Andermatt and Göldi [19] show that the availability of e-services linked to eID is of importance when deciding whether eID is useful for the citizens.

Awareness. The following category includes such expressions mentioned as "understanding" [40, 55], "seeing reason/purpose" [75], "knowing how to use" [22], "comprehending". [22] indicate "awareness" in the context of knowing how the systems works and knowing how to use it and connects this notion to the trust. In [115], Tiits et al. suggest that awareness of, for instance, technical aspects of a currently implemented solution will not guarantee the acceptance of future updates and changes, which implies the temporariness of such attribute.

Control and empowerment. The given category refers to "control over eID (or e-identity, or identity)" [54], "empowerment of citizens" [7, 12, 40, 43], i.e., their ability to choose whether to use eID, which personal data to provide, ability to check the status of data, ability to withdraw data, participation. In [40], Chauhan and Kaushik mention "empowerment" in the context of citizens being able "to access their information without "bureaucracy". In the work of [12], authors use "empowerment" as a reference to access to services, more precisely "so that they can legally control service delivery to their advantage." In the work of Halperin and Backhouse [54], "control" appears as a major theme during analysis of primary data and concerned control of citizens over their personal data as well as the issue of data integrity and disclosure by consent.

Transparency. This category generalizes the understanding of underlying principles of how (accountable) the data is being handled in legal, administrative and procedural sense by authorities [7, 125]. In [12], Al-Hujran et al. define "transparency" as a result of a process of "bringing visibility to citizens of the service workflow by means of automated service delivery." The comparative study on citizen perceptions of eID and interoperability provides a formulation of "transparency" given by a citizen as "ALL data that are collected about me should be made available to me, so that I am able to recognize who has collected what data about me." [54]. In the work of Al Marzooqi et al. [13], the context brings up "transparency" along with the approach organizations handle data with.

Path dependency. This particular category that somewhat represents rather a different perspective than the citizen one, yet it was introduced due to the arguments in studies of Brugger et al. [35] and Melin et al. [81] justifying the fact that paths chosen by countries and the previous setting they possess (including societal) when introducing eID are definitive for the stakeholders' perceptions (including end-users, i.e., citizens).

Path dependency refers to "previous technical, organizational and regulatory settings explain for the differences in the provisioning of national eID systems and thus the heterogeneous landscape of solutions and usage across Europe" [35]. Within the current study, path dependency is defined as rather an external factor of influence that has not been articulated by end-users. In [81], Melin et al. highlight the need of understanding the scenarios that worked out successfully in one country's case and did not prove itself when applying the same strategies in another country. Authors then state that citizens have a major potential to determine the outcome of each scenario. Hence, they suggest exploring more deeply eID introduction in the socio-material perspective, i.e., citizens' relationships with eID artefacts.

Cultural and historical factors. Five studies have provided insights on the role of culture and history in shaping citizen perceptions and acceptance of eID [8, 12, 35, 52, 13]. An elaborate opinion on how historical events can have a major impact and shape the sense of identity is given in the case study of the Hong Kong eID by Goodstadt et al. [52]. In the rest of the studies, history and culture appear as a background to the main narrative [8, 12, 13, 35].

The categories of "privacy concerns", "security" and "trust" are the most voluminous within this study [V]. All three notions are seen as issues to be leveraged in order to increase their trustworthiness in the eyes of the citizens [35, 54, 23], [VII].

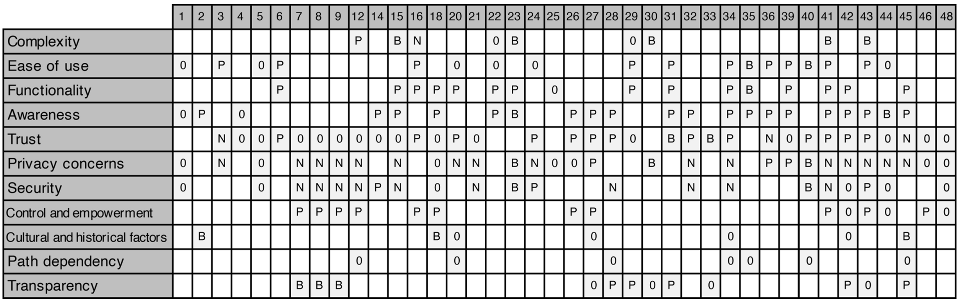
Privacy concerns. Notions related to this category are associated with risks, fears, threats to citizens' rights which can be applied in relation to their digital identities [55, 22, 50, 133].

Security. Here, the identified notions are related to data, software, and hardware, their reliability, trustworthiness, safety, and the ability of the state to guarantee this security [62, 23, 22, 38, 40, 79, 98].

Trust. This category is the most prevailing one. Even though we do not make any claims about the degree of influence that each identified factor has, trust has been seen and presented by researchers as one the most important pre-conditions of eID success. Trust is interrelated to most of the other categories and could be divided into subcategories or appear as a standalone factor. In the work of Lockton [72], "trust" is displayed a two-type concept that included institution-based trust and characteristic-based trust [134]. Here, the institution-based trust represents the trust that citizens experience towards public authorities and their activities, whereas characteristic-based trust is the one that end-users put in the system or solution. Another study by McGrath [79] identifies "trust" as well as "distrust" as two independent and separate sides of the same relationship and not as two opposites of one continuum. These two sides, as authors explain, co-exist and evolve as the relationship matures and evolves over time. Here, term 'relationship' is used in the socio-technical and political context. Therefore, ambivalence is the main attribute and finding regarding trust and distrust that varies from country to country clearly influencing the development outcomes.

Other. This category includes notions that have not been assigned to the abovementioned categories. One of the notions is the 'intrinsic motivation to adopt the technology' (i.e., eID) [55]. The same source has identified cost and expenses associated with the use of eID as an influential factor. Another aspect is the extent to what the technology has to spread before the user will actually start adopting it him or herself. This tendency particularly echoes the diffusion of innovation theory where such users are known as *late adopters* [103]. Lastly, the survey conducted within the study of Goodstadt et al. [52] has also identified as an impact factor the citizens' possibility to receive help from a competent person when using the technology, or in other words, technical support.

Backtracking, the issue of cost was raised also in [35]. In [16, 14], Alkhalifah and D'Ambra proposed a model with six key elements that affect the adoption of identity management systems, one of which – 'individual differences' – was distinguished as a notion in our research as well. The element of 'individual differences' is then divided in two sub-elements: demographic variables and situational variables that both have direct and moderating effects. The demographic differences include gender, age, and education as characteristics of individuals and the situational ones are referred to as context-sensitive characteristics, i.e., experience, facilitating conditions, subjective norm and cost. A study on the acceptance of biometrics in identity management [60] revealed that "age, gender, education level and occupation do not influence the respondents' views on the acceptability of biometric identity databases in any considerable way." In [81], Melin et al. mention such factors as eID user maturity and national differences in perceptions of information sys-



	1	2	3	4	5	6	7	8	9	12	14	15	16	18	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	39	40	41	42	43	44	45	46	48
Complexity										P		B	N				0	B						0	B									B		B				
Ease of use	0		P		0	P							P		0		0		0					P		P			P	B	P	P	B	P		P	0			
Functionality						P						P	P	P	P		P	P		0				P		P			P	B		P		P	P			P		
Awareness	0	P		0							P	P		P			P	B			P	P	P			P	P		P	P	P	P		P	P	P	B	P		
Trust			N	0	0	P	0	0	0	0	0	0	P	0	P	0			P		P	P	P	0		B	P	B	P		N	0	P	P	P	P	0	N	0	0
Privacy concerns	0		N		0		N	N	N	N		N		0	N	N		B	N	0	0	P			B		N		N		P	P	B	N	N	N	N	N	0	0
Security	0				0		N	N	N	N	P	N		0		N		B	P				N				N		N				B	N	0	P	0			0
Control and empowerment							P	P	P	P			P	P							P	P												P	0	P	0		P	0
Cultural and historical factors		B												B	0							0							0						0			B		
Path dependency										0					0								0						0	0			0					0		
Transparency							B	B	B													0	P	P	0	P		0							P	0		P		

Figure 8: Interpreted factors of eID public acceptance derived from SLR [III].

tems [V].

The identified notions within the created categories were interpreted in terms of their effect on the eID public acceptance. During the second level of analysis, each document item was analysed in order to identify the context in which the notion (or factor) is spoken of by the authors. Each category within a document item was assigned with a "quality" that signifies the effect on eID. In other words, a notion is presented as a driver or a barrier. Moreover, the impact of a factor, as it was learned from the narratives of authors, may range and hereby it can be assigned to both positive and negative group. Lastly, some derived factors were contextualised neither as positive nor as negative. Additionally, some analysed documents elaborate on the factors in a neutral context by not implying their positive or negative impact but merely assuming the possibility of impact if any. The conducted interpretation can serve as a guide to the identified factors and allows for an in-depth understanding of the factor's nature within a certain context and hence, can be considered as on the of the contributions of this dissertation. Additionally, it can help navigating through the conducted SLR. Figure 8 shows the interpreted factors of eID public acceptance derived from each literature source included in the SLR. The number in the top of the columns indicate the number of literature sources listed in Annex []. The list of literature sources is taken from the original published SLR [III].

At the moment of finishing the synthesizing the results of this SLR in 2019, the derived categories were presented in the published work [III] as potential metrics for assessing the acceptance of eID. Later, in the course of further research activities within the current dissertation, the idea of taking further the derived categories as variables that could be quantified and respected as a set measurements or metrics was dismissed. Instead, the focus was shifted on the qualitative aspect these identified factors can shed light on in the pursuit of answering the research questions of this dissertation. As we mentioned in the published work [III], the limitations could be the issues associated with this particular study that may influence its validity, is subjectivity that may have affected the analysis of the retrieved literature sources. However, the input of this study was incorporated within current work and delivered compelling evidence of its applicability. We will be further discussed in Chapter 6.

5.3 Attitudes and Perceptions of eID

This section is adapted from [V], previously published by Springer. It reports on the third data collection. The procedure and methods used are described in Section 2.2.

The aim of this study was to investigate the preferences of Estonian citizens when it comes to authentication option and hence get an understanding what are the eID pub-

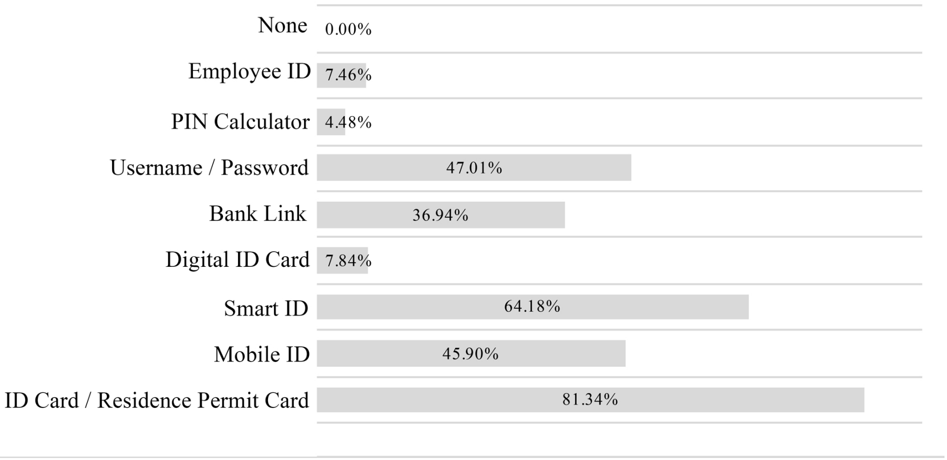


Figure 9: Types of authentication options used.

lic acceptance factors specific to this country. The set of factors previously defined by means of literature review was used as a part of theoretical framework for designing the survey as well as for the interpretation of results. 268 responses were collected. The survey was created in the online platform surveymonkey.com. Social media platforms and email channels were used to distribute the survey. The survey was distributed in three languages: Estonian, Russian, and English. The survey consisted of 12 questions (see Table 10).

The survey questions have covered such aspects as eID as a point of access to e-services, frequency of use, purpose, preferences for authentication options. When asking about e-services and their use we have distinguished between those provided by public and private sectors. To have a more detailed picture of what makes eID attractive for daily use, questions on features and functionalities were posed. Respective questions were also asked to explore current attitudes towards eID and their sense of trust.

The aim of the first two questions was to collect demographical data about respondents. 50.7% of respondents are male, 49.2% - female. The age groups are represented as follows: 32.4% (87 respondents) - 18-24 y. o., 32.8% (88 respondents) 25-34 y. o., 22.7% (61 respondents) - 35-44 y. o., 7.4% (20 respondents) - 45-54 y. o., 1.8% (5 respondents) - 55-64 y. o., 2.2% (6 respondents) - older than 65 y. o.

Then, the respondents were requested to choose which of the existing authentication methods they use when accessing e-services. Figure 9 shows that the ID card is used the most frequently among the respondents. Smart ID follows. Username and Password is the third-choice option - 47%. Mobile ID reaches almost the same number - 45.9%. The respondents were able to choose multiple options. The statistical data provided by SK ID Solutions, Estonian Certification Authority, on the number of OCSP requests made with Smart ID and Mobile ID (see Figure 10) shows how in the matter of months after its launch Smart ID usage overran the Mobile ID. Ever since 2019, the numbers of Smart ID usage have been continuing to increase.

Next, the respondents were asked to specify how often they use e-services. 50% of respondents stated they are using e-services on a daily basis. Around 29% reported at least several times a week, 8.9% - once a week, 9.7% - a few times a month, 1.8% - once a month, 0.7% - less than once a month. None of the respondents reported not using

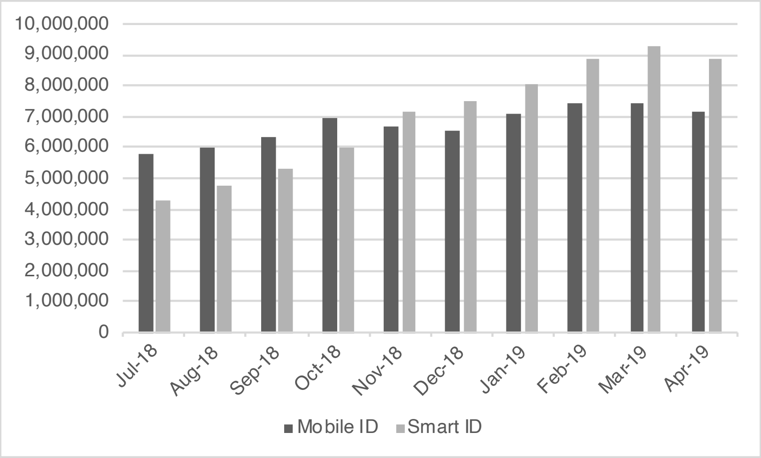


Figure 10: Number of OCSP requests.

e-services at all.

Since there is a great variety of e-services, respondents were asked to specify which ones they access by means of available authentication options so that the ratio of public and private services could be clarified.

Four types of services such as financial, healthcare, education, and transportation e-services were clearly distinguished based on the responses. The e-services provided by private sector that require authentication are listed and grouped in categories such as transportation, entertainment, lifestyle, food delivery, telecommunication (e.g. mobile phone, internet), financial (e.g. banking). The results revealed the following numbers: transportation – 70,1%, entertainment – 60,4%, lifestyle – 78,7%, food delivery – 47,7%, telecommunications – 87,3%, financial – 90,6%.

Respondents were asked whether there were cases when the preferred authentication option was not available in a particular e-service. More than half of respondents, 56,41%, confirmed such cases occurred while the rest 43,5% replied negatively. Those who could not authenticated themselves were asked to clarify what was the service they had tried to access. 63% indicated it was a public service (e.g., many educational institutions do not support Smart ID yet. There are also occurrences of technical issues when using ID card or Digital ID card). The rest 36% of respondents reported private services not supporting their preferred options (e.g., a large number of private sector service providers do not support eID-based authentication).

The respondents were asked to explain their choice and preferences when using a particular authentication option. The responses were textual and hence thematically analysed after which grouped into themes. Each response was coded, and the themes were formed. Many responses combined more than one code, so they are presented separately as combined themes and nodes (see Table 9).

Respondents were able to choose from authentication options. Smart ID, Mobile ID, and ID card ranked the highest. Many of the submitted answers contained an indicated authentication option together some of characterizing factors (see Factors block in Table 9). For example, Smart ID + Convenience was mentioned three times; Smart + Mobile ID - four times. A triple combination of Convenience, Speed, and Security was mentioned relatively frequently as standalone theme and as its variations of double-factor combination. Convenience appeared as the most frequently named factor prioritized by the

Table 9: Most frequently mentioned features (Adapted from [V]).

	Position	# of times mentioned	% from total # of respondents
Factors	Convenience	41	18
	Convenience + Security	17	6
	Convenience + Speed	27	10
	Convenience + Speed + Security	7	3
	Security	8	6
	Speed	16	6
	Security + Speed	5	2
	Ease of use	10	4
	Usability	2	1
	No additional device needed	5	2
	Availability	5	2
Nodes	Convenience in total	101	38
	Security in total	38	14
	Speed in total	65	25
Authentication	ID card	20	8
	Smart ID	45	17
	Mobile ID	24	9
	Username/Password	5	2
	Social media account	2	1
	PIN-Calculator	1	0

respondents.

Further survey questions were asked with an intention of understanding what potential features users are open to when it comes to authentication. Users were offered to chose from a list of verification factors. The majority - 78.36% - of users indicated willingness to use fingerprints. With respect to other biometric factors, 28.73% chose iris scan, 27.61% - facial image recognition. Voice recognition appealed to 11.94% of respondents. Around 40.30% - would like to use NFC (Near Field Communication) technology. As a matter of fact, it is worth to note that as of 2018, a new generation of Estonian eID *smart cards* are issued and NFC feature is supported [107]. Three respondents marked refusal to use the suggested options referring to distrust.

Respondents' opinion was asked on whether there are enough authentication options available. Almost 74% agreed there are enough, around 20% would like to have more, 3% marked there should be less, and 3% replied with "I don't know."

The question on the opportunity of having one universal solution gained similar results where 64% of respondents replied they would like to have several authentication options available, almost 28% found the idea of having just one option to be appealing, and around 8% indicated they do not know. A few respondents commented that there has to be more than one option available. One of the respondents found the idea of a universal solution to be "utopian", and the others mentioned that considering the existing problems with eID, it is better to have alternatives. Also it was noted that having only one option would result in more risks and security concerns.

To understand, how trustworthy the authentication options are, the respondents were asked if they trust the service providers to process their personal data. About 20% of respondents marked that they fully trust the service providers. The same number of respondents noted they do have trust but some concerns exist. 36% felt skeptical but nevertheless continue to use eID and e-services. About 3% expressed they do not trust and feel concerned about their personal data. Lastly, the same number of respondents shared that they do not understand how their personal data is processed and what the implications may be.

Furthermore, as a part of data synthesis in this study, the results of analysis of this data collection round are discussed through prism of previsously identified eID public acceptance factors (see [III]). The below interpretation is adapted from the previously published work (see [IV,V]).

Complexity. This factor explains to what extent users perceive the solution at use as a difficult-to-use system [102], [III]. During the analysis of survey responses, no results were linked to this factor since the focus of this data collection round was put on the factors that make the solution appealing to users.

Functionality. This factor refers to the perceived usefulness and benefit [45]. The results optained allow for a conclusion that the respondents value efficiency, practicality, and usefulness of authentication options and e-services that are available.. 25% of respondents marked speed as one of their priorities when they choose which authentication option to use.

*Awareness.*The analysis of submitted textual answers revealed that the respondents are knowledgeable and tech-savvy. In their answers, many respondents demonstrated awareness and consciousness about potential risks when it comes to security and privacy, capabilities and limitations of the existing system, principles of its functioning, etc. For example, one user has mentioned the following about having one universal authentication option:

> *"The issue of technical capability. One central convenient working system would certainly be more convenient. However, given ID-card authentication issues, this problem would be greater if alternative authentication tools did not exist."*

In [23], Backhouse and Halperin point out the awareness to be one of the bridges to understanding, trust and, hence, user acceptance. Additionally, Chauhan and Kaushik [40] argue that a lack of awareness can lead to a perception of the technology as too complex to use. The activities aimed at increasing awareness of Estonian population about opportunities the use of eID and e-services were effective judging the growing numbers of users and the volume of services provided [90, 83].

Control and empowerment. This factor refers to the citizens' ability to control his or her personal data and access to it [III]. Moreover, it includes issues related to disclosure by consent, data integrity [54], access to services [9]. The analysis of data collected within this research round did not show results relevant to this factor but is sufficiently elaborated on in our study [VII].

Transparency. In the context of authentication options, this factor refers to citizens' ability to understand how his or her data is processed by service providers and how the solution works overall. In other words, if the user the minimum level of understanding required to be able to use the solution, i.e., in this context, the authentication option. Transparency is also characterized as the visibility and accountability brought to citizens through the service delivery [9]. In the survey, the answers to the question about respondents' trust to the service providers who handle their personal data revealed that only about 4% of respondents who do not know or do not understand how their data is being handled. although within this data collection and research round, this part of results seems to be the only aspect discovered in regard to transparency factor, the given number presents this aspect in a positive light.

Trust. Whether it is public or user acceptance, it heavily relies on users' trust towards technology. In the public sector, the concept of trust applies not only solely to the technology but to the service provider who must show their integrity by ensuring proper personal data processing. Within this research round, 20% of respondents replied they fully trust the service providers in handling their data, 19% demonstrated some concerns, 36% felt skeptical about the matter, and around 4% showed themselves to be highly concerned;4% replied they are not aware or do not understand how their data is handled. Therefore, it may be concluded, that generally, in Estonia, the level of trust is relatively high. The matter of trust will be discussed in more detail in Section 5.4 when reporting on the results of the fourth data collection round.

Privacy concerns. Privacy is tightly linked with the factor of trust. As privacy concerns comprise risks, the latter go hand-in-hand with trust [22]. There is no consensus on how they are related. A study of Sjöberg [110] revealed that trust is underpinned by the perceptions of risk. In the context of this research, as was stated just above, respondents reported on a certain amount of distrust towards the service providers. For example, the below comments were submitted where the following was mentioned:

> *"Don't trust to e-elections"*

> *"I trust public sector, and I'm skeptical of private sector."*

Other technologies, for example, biometrics, that are used in identity management field, are associated with risks [60]. The respondents expressed they willingness to use biometrics but some shared the following opinions:

> *"I have concerns about some of the abovementioned options. In particular concerns about security and reliability of those, especially given the modern technological advancements in AI (image rendering; voice reproduction). Hence, perhaps the only reasonable option is iris scan."*

> *"Prefer non-biometric options for privacy reasons but don't feel current tech allows for needed security. Smart ID is the best currently available in my opinion"*

> *"I would only use fingerprint if it were an "additional" layer of security, not the only authentication needed to log in."*

The raised concerns remain relevant. As [53] note, the concept of trust has been in focus of research in eCommerce primarily, where the trust of consumers is directed toward vendors not known previously, a situation of "initial trust". In such setup, a predisposition to trust is already in place. However, Sjöberg [110] argues that, in the public sector, the citizens, or "consumers" of the public services, are already too familiar with the service provider, i.e., the state. In this sense, the technology itself is not an object of (dis)trust anymore but rather becomes an issue related to the service provider that citizens do not find sufficiently trustworthy.

Security. This factor reflects the state's, i.e., the service provider's, ability to establish, maintain and guarantee the security of data, infrastructure, ecosystems, and their integrity. The importance of security is almost impossible to overestimate so it does not come as a surprise that the respondents prioritized the issue of security when choosing a suitable authentication method. Security was mentioned in total 38 times. It will be discussed further in more detail in the context of the results of the fourth data collection round and the overall discussion.

Ease of use. This factor has been defined through many authoritative theories as a major one when it comes to the public acceptance of technologies [45, 130]. Davis defines ease of use as the "the degree to which a person believes that using a particular system would be free from effort" [45]. In this round of research, the convenience (or ease of use) was the most frequently brought out subject by the respondents. As Table 9 shows, it was mentioned as a priority more than 100 times. In [40], Chauhan and Kaushik also mark convenience as one of the motivation factors of the eID acceptance. In [34], Brown indicates that "the ultimate convenience product or service would then be available continuously (time), everywhere (place), and would require almost no effort to acquire or use." [34].

The results of the survey determined the ID card, Smart ID, and Mobile ID as the most popular authentication methods. Since it was possible to choose multiple authentication options, most of them were ranked by the respondents. In this regard, several points can be made. Firstly, the available authentication options can be used in parallel with no conflicts. Secondly, at least half of the respondents marked they are using e-services on a daily basis, and around one third marked they do so several times a week. This means a high number of active users with large volumes of transactions. The given aspect will be also mentioned in Section 5.4 where the results of fourth data collection round will be presented. Thirdly, given that e-services are provided both by public and private sectors and the authentication options may vary, it can be assumed that one person uses at least two options. A governmental portal may offer access to its services with ID card and Mobile ID while the same user will log in to an insurance company's self-service using Smart ID.

It is difficult to conclude which authentication option is ultimately the leading one. As results show, the respondents favor ID card, Mobile ID, and Smart ID. Other options have been gradually phased out. Respondents mostly agree that there is enough options available and having a universal solution most likely would not be a good idea. In 2017, Estonian e-identity management discovered a major security vulnerability known as ROCA (Return of Coppersmith Attack) that affected more than 70% of eID cards [VI]. Having at disposal alternative options perhaps was one of the key reasons that made it possible to continue run the digital state without major interruptions.

In the regard of ID card usage, a report of Buldas et al. on the lessons learned from this case states, the incident not only has not affected the eID usage, it has continued growing steadily since then. The State Information System Authority as well as the Police and Border Guard Board have prioritized to retain people's trust during the crisis solving [VI]. The amount of written answerts submitted with respect to Smart ID complement the numbers that show constantly increasing numbers of its usage and confirm its growing popularity among the public.

A study of Sai [106] on the adoption of Smart ID in Estonia postulates that the rapid growth of usage happened due to quickly spreading news through several large service providers, peer networks, and opinion leaders about availability of a simple, fast, and secure solution. Once again, cooperation of the private and public sectors proved to effective as an adoption stimulus [70], [VI].

5.4 The Role of eID Public Acceptance

This section reports on the fourth data collection round. The aim of this data collection round was to answer RQ3. Table 10 lists down the interview questions.

The thematic analysis of the interviews was conducted following the guidelines of Braun and Clarke [31] (see Table 6). It consisted of the following phases:

Table 10: Interview Questions.

Q1	In which field are you working? Is it related to eID?
Q2	Does your field of work depend on eID and its functionalities? How often do you use it to conduct your daily work-related activities? (every day, couple of times a week, couple of times a month, rarer)
Q3	How the public acceptance of eID affects the e-government success? What is its role?
Q4	Can you identify a few main aspects that contribute to the eID public acceptance in Estonia?
Q5	How citizen's level of trust affects the technology acceptance in Estonia? Is there such thing as minimal level of trust for e-government success?
Q6	What, in your opinion, has contributed to and accelerated the gradual process of the eID acceptance during the years after it was introduced? Can you identify any specific actions from the service providers' and other stakeholders' side?
Q7	Considering that eID became a part of the state critical infrastructure, how important is it for the citizens? Are citizens actually dependent on eID? (any particular sub-groups?) In your opinion, what are the main services, aspects, or functionalities that make eID vital for them?
Q8	[ROCA case] Who would immediately be affected? Which user group(s)? Could you explain why?
Q9	In Estonia, has the state has become the primary user of eID and the related infrastructure? Is the state dependent on it more than other users?
Q10	Do you think these integrations [ad hoc electronic workflows in organizations] strengthen eID acceptance? Should organizations be encouraged to implement it as a part of their internal processes? What are the benefits and opportunities of such integration? What are the risks
Q11	Do you think it is necessary to strive for lowering the number of those users who (almost) never use eID by raising their awareness? Is it a priority?
Q12	Should the eID public acceptance continue to increase? How can it be increased?
Q13	What are the future plans with regards eID? How e-services can be improved so that eID will be used even more?

Phase 1: Familiarizing with the data. The interviews' text was reviewed thoroughly.

Phase 2: Generating initial codes. The first round of coding was conducted and initial codes created.

Phase 3: Searching for themes. Five initial themes were created. The hierarchy of the code tree included four levels. The total number of codes identified at this stage was 87. The number of individual references was 1334.

Phase 4: Reviewing themes. During this process, the codes and themes were readjusted keeping in mind the research question #3 as the primary one while arranging the codes according to the narrative that contained possible answers for the rest of the research questions, #1 and #2 respectively. Some of the codes were deleted, some merged. As a result, four final themes were identified. The fifth theme was not deleted but was rearranged to hold the codes which contained indirect and/or complementary information on the subject of the study. Eventually, the total number of codes was 66, while the number of individual references – 1247.

Phase 5: Defining and naming themes. The final adjustments within each identified themes were made. The final themes' names are: 1) Public acceptance, its role and factors, 2) Acceptance level, pervasiveness, 3) eID concept, 4) Actions and Decisions (see Figures 11, 12, 13, 14).

Phase 6: Producing the report. In-depth analysis of the final set of coded references was conducted. The analysis report that contains of main highlights is presented further below. The report reflects on the insights received from the informants, however, the holistic answers to all research questions will be presented in the Chapter 6 in order to include inputs from all data collection rounds.

A note should be made on the description of the themes. In order to maintain the flow of arguments, facts, and the narrative overall, the quotes of the expert interviews are given in their full and extended format. That way, the reader is able to get the most out of the story and put the presented thoughts and statements into perspective.

5.4.1 Theme: Public Acceptance, its Role and Factors

This theme holds features, attributes that contribute to and build public acceptance. These features and attributes are more abstract and general (see Figure 11).

The collected narratives from the experts joined in this theme contextualize the previously defined factors of eID public acceptance within the case of Estonian eID.

The codes created within this theme are based on the factors defined in the previous study [I]. The following ones overlapped with the factors: Awareness, Convenience, Privacy and Security, Trust. The references were coded using top-bottom or deductive approach. The codes Availability, Inclusion, and Motivation were created based on the frequency of mentioning those by the experts. Here, a bottom-up or inductive coding was used.

Below we elaborate on each of these codes.

5.4.1.1 Availability The narratives on the availability of e-services that hence be accessed with eID prevail. The availability entails inclusivity and equality, i.e., everyone has the right for the service as well as the possibility to access it.

One of the informants mentions:

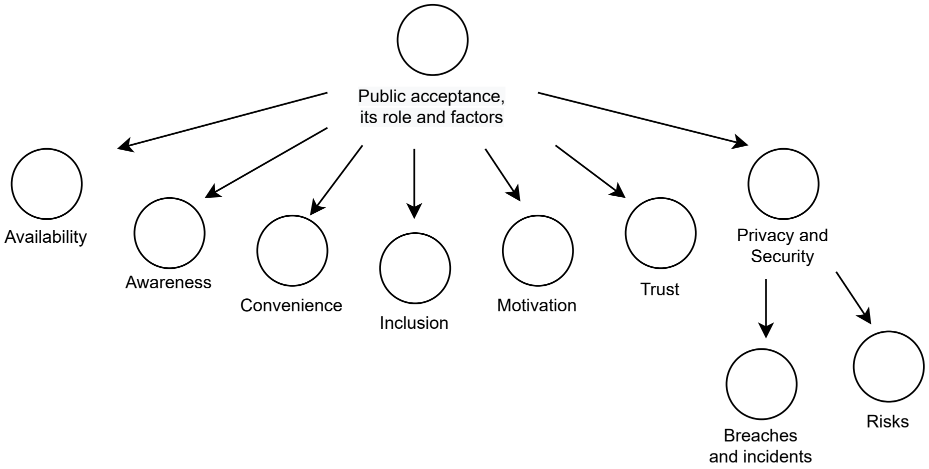


Figure 11: Theme "Public acceptance, its role and factors".

> *"It might be also policy and political question: how to enable equal rights of people to access"*

He also then gives a follow-up:

> *"[. . .] many places in Estonia still were not so easy to access internet, and, of course, most people are not, even if they know how to use those services, they are not always able to do it; and this is another policy that shows how to enable all people to access"*

Two informants noted the gradual process of e-services' growth that correlated with the use of eID. One of them mentions:

> *"Because when we started in 2002, and in the beginning there was a good attitude from the public sector. In the media, they would take card as useless. There was no e-services. "Why we need that kind of card? Why we spent so much money for that card?" But we still continued to issue the cards and now we can see, okay, now, it's been sort of like 10 or 15 years ago, we saw that, okay, e-services are coming and there are a lot of benefits for that card."*

It also has to be specified that during the roll-out of eID, according to one of the informants, there were already e-services existing and could be accessed via bank-enabled authentication means. Yet the number of these e-services was rather low. The correlation between the eID and e-services calls for a question: which enables what? What needs to be implemented first to start the process? Three informants named it a "hen-and-egg " question. They all replied to it that there is no way tell but what is clear, is that both have to be done.

This code is very similar to the code *Inclusion*.

5.4.1.2 Inclusion Within the acquired narratives of informants, the aspect of inclusion refers to ensuring that each and every citizen is covered by the overall service provision and is given the possibility to use the service(s). Here, the inclusion can be also looked at from the perspective of multiple user groups and the equal possibilities provided to them.

Keeping in mind a relatively high level of e-services maturity, eID, and their stability, the informants were asked whether it is required to strive and put effort into increasing the use of eID [IX].

One of the informants answered:

> *"Every single citizen that lives in Estonia is of interest to the government. Which means that it is definitely important for us to reach also the users that are not maybe on board with eID. But at the same time, in a sense, yes, I think it is necessary to lower those numbers, because we want these conveniences for everybody"*

The other informant though believes it is only possible to reach a certain level of users (70%), while the rest of them cannot be covered. According to him, a large number of users still own simple cell phones, might not have a PC, or just choose not to use any of the eID options.

Among these mentioned 30%, children who have not turned 16 y. o., might not own an eID card. Those who might, use it as a travel document. There is no intention to impose the eID and e-services and leave freedom of choice:

> *"[. . .] if someone is not using it – it is an individual decision of that person and, well, no problem here."*

The answers of informants come to a point were inclusion has to be reached genuinely through invoking the wish of the people to start using eID. One of them mentions:

> *"I think the way also in Estonia, how to get more people to use eID and how to use the digital solutions should be just making it better and better."*

> *"[. . .] the user-centered approach of developing services is the best tool for getting people to actually use those"*

Additionally, when talking about inclusion, and, as a matter of fact, availability, a remark was made on the language of the services provided. Since a large part of the citizens in the country speak Russian, and more and more people who speak English as their primary language come and settle in the country, a demand for multi-lingual support in service provision is appearing. One of the informants noted, that part of the services is provided only in Estonian language which often becomes an issue to those who speak other languages. Looking at it from solely citizen experience's point of view, this can lead to a certain degree of disappointment and frustration on the citizen's end. Therefore, inclusion and availability can consist of many nuances that have to be kept in mind in each specific setting in order to provide equal opportunities for everyone. Moreover, the language is also used here as a tool to convey meaning. The simpler it is, the easier for all people to comprehend it:

> *"[. . .] because we found that also many service portals are very complex. So people like simpler things. It's also about how you are using language. To reach some Ministry of Justice portal, you can read some very legal language [. . .] "*

5.4.1.3 Motivation From the experts' perspective, motivation appears to be a highly important factor. Motivation can be reached primarily through useful services. Importantly, there should be a variety of services available. Indeed, it requires a certain amount of time for the services to become available, but the key is rather to have multiple initiatives to carry on, implement and demonstrate the benefits. Motivation is there if people find it useful. The purpose is what drives the usage, as the experts argue:

> *"[. . .] if you get a tool to access governmental services, and you can use it only once a year to declare taxes, of course, you're not interested. Even if you this tool, after one year, you forget how to use it."*

> *"[. . .] if the person doesn't use it, the issue is not on the electronic identity side, but basically, on the services that are provided to them. And they don't find the service that would make them use it."*

> *"[. . .] If you want to get people use the services and solutions, those have to be of good quality. So if someone it not using, either he or she has no use for the solution, or it is not good enough, if it is beneficial, I'm sure they will use it."*

It may seem that the focus is slipping from the eID to services but a reminder is that these two concepts are inextricably linked to one another. One cannot function without the other. eID is a tool and enabler of service provision as services cannot be provided to the citizens while skipping the their identification. On the other hand, if no services are available, too complicated, or unknown, the eID then has little to no value.

> *"[. . .] everybody should take very seriously about motivation of people start to use it. Otherwise, you can build fancy good ID system but nobody is using it."*

> *"I think the way also in Estonia, how to get more people to use ID an how to use the digital solutions should be just making it better and better."*

5.4.1.4 Awareness This code matches with the previously identified factor of awareness. It refers to users knowing that a tool or a service exists, can hold value and benefits, and is possible to acquire. Reaching awareness is a process that may require a large number of actions to continuously boost it [VII].

The informants reflected on a few projects commenced in late 1990s – early 2000s which goal was to get people familiarized with the internet and educate them to use a PC: "Tiger Leap", "Look at the World", and "Computer security". These projects were aiming at covering different age groups – from children to elderly. The informants also mentioned IT buses as one of the ways to increase people's digital literacy.

Several informants pointed to an initiative on using eID in the public transport by the elderly. The idea was not use it as a ticket, but the motivation factor was to provide a twenty-five percent discount to pensioners when purchasing a bus ticket.

> *"And then we came out with the ticketing for the public transportation where it didn't have to have a paper ticket. You didn't have to bring your pensioner certificate or anything like that, you just showed your ID card, then somehow, magically, the check could be done that you have a ticket. And because elderly people could buy a bus ticket that actually didn't cost them much, or actually nothing, if you were over 65. That was days for elderly people, they understood they need the card."*

A further comment was then made by the same informant, the author of the quote right above, to explain why it was considered as an effective initiative:

> *"It was clearly one of those kind of mass services you can think of, that very quickly got traction, because you really didn't need to kind of learn much, you didn't need to have a device, you went to a small booth and ask your ticket to be connected with this card."*

Considering the outcomes of interviews from the first data collection round (see Section 5.1, a specific instrument for raising awareness was used in a form of marketing government services by means of advertisements. One of the informants argued that awareness comes through communication rather than advertisements. Advertisement can be a part of a tactic to raise awareness but more importantly:

> *"The communication, which is always required, that you have to communicate, yes, now we have the solutions, now it's available for anyone, and to communicate the benefits. Why one should use it? What is the benefit one gets from it?"*
>
> *"[...] when more and more people use it, and can say that their experience is positive. Well, it's bringing in new users. But I do not believe in the power of advertisement, because in the end, they will however, use the solution and see if it is good or not, it can raise awareness. Well, that's the way how the advertisement can help."*

Summarizing the comments of experts, awareness is a result of deliberate subtle actions of stakeholders and an outcome of the implications of those actions. While on the stakeholders' end it requires a structured and consolidated approach to delivering the solution as well as the necessary information about it. The latter includes projects, public campaigns, announcements that will send the message about the solution, create its positive image and eventually converts the new knowledge about it into users' desire to use the new solution and receive its benefits.

5.4.1.5 Convenience Convenience code overlaps with the factor of ease of use. It also corresponds with the "ease of use" variable that constitutes the technology acceptance according to the TAM.

Convenience is commonly acknowledged to be one of the most important factors articulated by the users. The interviewed experts note it as well to be the main driver and requirement coming from the end-users' side. The Chief Technology Officer (CTO) of Estonia argues:

> *"the most important role of technology is to automate routines in our everyday life, so that we could save time to spend time with our friends and family, or do whatever we want to do, including being lazy. This is perfectly fine. And I think that if we create technological tools that make inconvenient stuff more convenient to people, then this does contribute to public acceptance."*
>
> *"once you show that people are saving time, I think this definitely contributes to the public acceptance."*

Also, the informant who wished to remain anonymous seconds the previous statements:

> *"I consider the important factors to be the easiness and the way how people actually experience it."*

One of the detected narratives related to convenience appeared to be multiple platforms of eID. The distinguished ones by the experts are the Mobile ID and Smart ID.

More than a decade ago, a boost in the usage of eID was clearly seen after introducing the Mobile ID. The CTO of Estonia reminisces the following:

> *"I think that mobile ID was a huge kick, because it made your digital identity very convenient."*

He then adds:

> *"[...] there's a very specific correlation that shows that if you made your digital identity even more convenient, by enabling it through your mobile device"*

He then also continues with the Smart ID believing it is now having the same, if not larger, impact on the public acceptance of eID due to how well it caters to the users' needs. As a conclusion he summarizes:

> *"This is the most important role of technology, you have to find places where you can create a more convenient environment for your citizens, and then they are more happy to be in this environment. So I think this was really, really important."*

It is important to note that the matter of convenience was discussed during the interviews not only from the perspective of authentication options. eID can be used for enabling electronic workflows in the organizations. Therefore, such integration allows for receiving the benefits eID can provide in such setting: high security level, ease of use, universality and free access to the technology behind. Implementing the eID functionality in the back-office systems of governmental entities contributed to the public acceptance of eID from the service providers' side as it simplified their work routines and made them more convenient. More on this will be discussed in the description of the theme "eID concept".

5.4.1.6 Privacy and Security A number of issues has been discussed within the current code. The references under this code contain the view of experts on the issue of privacy and security and its importance for eID public acceptance and how this issue being a part of the public acceptance affects the overall success of eID. The main issues raised during the discussion with the interviewed experts were sorted to the sub-themes: "Risks" and "Breaches and Incidents".

The privacy and security aspects discussed during the interview are broad as they cover several matters of eID: concept, infrastructure, functionalities, use cases, and users. All of the experts unanimously agreed on the high priority level of this particular aspect, i.e., privacy and security, and on the challenge of assuring it ubiquitously.

The issue of risks was discussed in detail. Risk can be defined as a combination of likelihood and consequences of an unwanted event or cause that might result in damage and/or loss.

While risk itself is perceived as a negative phenomenon, it can be helpful at the same time. Being aware of possible risks, the possibilities of their occurrence, and the implications they cause is beneficial while designing, developing, and maintaining an information system.

The interviews with experts revealed a long list of risks they consider to such. The common sense appears to be, according to the interviewees, is that the highest risk so far is the lack of knowledge. Human factor and a low level of digital literacy, cybersecurity and cyberhygiene can have a far greater impact than a vulnerability of a system. However, risks in general are to be found in each part of the system. One opinion was submitted by the expert who wished to remain anonymous:

> *"I still consider the weakest point always to be the end Information Systems, because it involves a big number of information systems, a big number of people having an access to those Information Systems. It includes storing information, it includes log files which might also include some data actually, not just their like operational logs,*

> *but logs, which really have certain user data included. So it's multiple data sources with eight information systems and thousands of risks related to the information system."*

He believes that eID itself is much more secure, and other experts also supported this claim that a card does not need to be ultra-sophisticated. It actually has to be quite simple and elegant in its design while the software is the one which is supposed to be "smart". Now, the chip vulnerability discovered in 2017 is naturally a topic relevant for discussion in this context so it will be surely brought up multiple times further within this dissertation.

One of the interviewees noted that, for example, banks eagerly implemented eID within their systems for its security: while there were successful attempts to hack into the system using other channels, eID proved to be secure enough and no break-ins have been detected.

Here, the technology plays an important role. The digital signing capability enables a high-security assurance level which in turn is a motivation factor for the government. But this being just one part of the equation, what is also important is the user and his understanding of security principles:

> *"You're quite sure that this is a secure system, because it's kind of a security infrastructure. Security infrastructure doesn't guarantee your security without your own conscious mind."*

> *"And for the government, is another thing, the higher level of security – the more trustworthy system. And therefore, considering this, we have decided in Estonia that the government has to give a solution that works everywhere, it means that it has to have a highest level of assurance and technical security. That's the key."*

Overall, experts agreed that there is a strong dependency on the attribute of security which, if weak, creates a long list of risks of breaches, leaks, and other incidents. If privacy and security is not ensured, it leads to distrust and lose of users. The aspect of risks is discussed further in the current sub chapter, as well as the ROCA incident as one of the major vulnerabilities identified recently in the Estonian eID. It is followed by the "Trust" code and factor description rounding up the theme "Factors of public acceptance: its role and factors"

Additionally, in terms of risks, the possible implications of eID ecosystem failure were discussed. One of the interview questions directly inquired what is the most vulnerable spot in the system that would immediately suffer if some part got compromised. The question was also framed with a reflection on the ROCA incident. Most of the experts noted that it is difficult to point out just one system or aspect arguing that potentially such sectors as banking, healthcare, and the technical infrastructure itself would provide an immediate response to a possible failure.

A curious statement was brought up by the Estonian CTO who believes that at this point the likelihood of a major failure occurring and having a paralyzing impact on the state's functioning is very low. Instead:

"[...] I think that this is again, akin to how software works as a whole. There's no situation with a software that ends up in a place where you say that, hey, we cannot use nothing here anymore. And if this is true with software, with operating systems, especially, for example, with open-source operating systems where critical vulnerabilities can be found sometimes, that are patched, or even with proprietary operating systems where, sometimes, you don't even know that there was a crash vulnerability, and this is magically going to be patched as part of Windows Security or whatnot, is that we can patch these things."

He then continued that at this point of the state of affairs in the information systems, most of the crises, breaches, vulnerabilities and other troubles are solvable once good risk management, communication and leadership are in place.

To conclude, another comment of the Estonian CTO can be cited:

> *"The benefit here is that while the electronic identity is incredibly sensitive and important and critical part of assuring our digital identity, in the way it is built, and, sort of, the algorithms it's based on, are not so complex, which means that they are open enough or they're easily patchable enough, that they don't require a replacement of a whole operating system. They require just certain tweaks or certain adjustments for the algorithm, and then everything is going to be fine with your keys. Because in the end, it's about your private key, it's being secured."*

To round up the subject on risks and continue the previous statement on PKI, it is worth noting the words of one of the experts from the Estonian State Information Systems Authority (RIA) (Riigi Infosüsteemi Amet) cautions about the single point of failure, which he believes to be the Certification Authority, SK ID Solutions AS. In terms of risk management, a single public key infrastructure authority may become a weak spot in the system. Having more than one would be safer but since the market is relatively small to fit more businesses, at the given moment, there will not be any changes.

5.4.1.7 Trust Trust has always been one of the primary conditions when it comes to the acceptance of technology. The definition of trust within the domain of e-governance and electronic identity is not agreed upon and is somewhat elusive and intangible. Its concept can be tracked through almost all the narratives on the implementation and success of most of the technologies, especially those in the public sector.

When talking to the experts during the interviews, the trust revealed itself as a multilateral phenomenon that can function both as a cause and as a goal. Five out of seven interviewees have agreed without any doubts that trust is an extricable component of electronic identity. The interviews allowed to distinguish the following: i) trust towards the technology of eID, ii) trust towards the devices, iii) trust towards the service providers, iv) trust towards the government, v) trust towards the citizens. All of these kinds of trust must be maintained and treated equally as important.

All of the interviewed experts noted that in Estonia, the trust level is very high in Estonia. One of the experts even highlighted that some people rather believe more in the story of the Estonian success but not really questioning whether:

> *"Well, is it really that safe in all cases? Is it that well-built? Are we in a sustainable way how we are building or e-governance solutions?"*

Here, the expert distinguishes the base the trust is built upon: a story side and the actual technology or the reality side. He agrees that the high level of trust is definitely a positive thing and either way is always built on a story. Moreover, people start to trust more if the story is repeated. On top of the story, the general public then builds its opinion adding to that the experience of using the technology. When these aspects gather up, people feel they have trust and thus satisfied with what they get.

Two experts expressed an opinion that when it comes to citizens' trust, people don't care in general. However, based on their answers it became somewhat clear that what is meant by it here is that working deliberately on building up trust does not make much sense. Citizens do not need to know a lot about what is going on behind the curtain of the state and its infrastructure. Naturally, nowadays people do know more since the digital literacy has grown significantly, but still it is the state is the primary party who is interested in the issue of trust. To reach it, the solution must be trustworthy for the state itself. Therefore, the state makes sure the highest possible levels of security are assured. What was done in case of Estonia, is that it was decided to involve a third-party certification authority that will be in charge of issuing the certificates. The latter originate from one root certificate creating a technical trust. Therefore, as one of the experts (RIA) argued, the banks began to accept state-issued IDs.

Another expert who believes that people don't care shared his thoughts that basically match the above said but in different words. His point is that trust was not an issue in the first place. He argues that back in the days, when e-government was under development, a more pressing issue to solve was the attractiveness of the technology. The expert talks about digital elections as an example where the first digital voter turnout was only around 2%. As he explains, this number is not a result of distrust but attractiveness in the first place. Hence, it is better to concentrate on the technology and its development using a joint effort of all parties and give it time.

Digital voting plays here an important role. The government CTO of Estonia brings to attention the following:

> *"I think that with eID, it's been really critical that the government trusts the digital identity; then fights for the security of it. Because if the citizen sees that, you know, government trusts my votes, my democratic votes that are being secured and authenticated by my digital identity, then if government does this, this, is the most critical level of trust you can you can have, then obviously, I can use this for other things, including banking, or including less sort of traditionally critical things such as using it as a client card or customer benefits card and elsewhere. So, if it's already accepted in the highest level of trust, then they're more ready to also use it in other fields of areas."*

If we remember the different kinds of trust spoken of in the beginning of this section, then assuming that at first there was no trust towards digital ID or other technologies, the trust did exist between people, institutions, and service providers. As the CEO of the Estonian Certification Authority explains:

> *"[. . .] in Estonia, the electronic identity was brought out in a way where this launch was coordinated and agreed by the private sector and public sector; and banks very much supported in the public messaging."*

So, if the banks who have already been trusted by citizens are vouching for the electronic identity solution that is issued by the state, this creates an image of reliability, security, and, again, trust. People then see that both service providers are interacting with each other through the use of technology while demonstrating the safety and convenience features that come along. The CEO of the Estonian Certification Authority then continues:

> *"Also, the telcos at the time, at least some of them had a very clear statement that the brand is connected to innovation. So they are bringing the innovation to the country. So I think that there were a lot of companies who were related to the image of technology, technologically advanced companies. And the services in the sense worked. So they actually provided something meaningful to the people. That meant*

> *that it wasn't just a big part of why we do innovative things, but it actually paid off on a daily basis. So that's, I think, where the trust came from."*

After that he added:

> *"I think that this kind of a development that happened throughout the 90s and in the beginning of 2007, it actually meant that you could see that if you go along with the technical changes, you are becoming more and more successful in your personal life as well. So I think this was proven on a daily basis that it makes sense to go there. So yeah, some level of trust was there."*

In other words, the Estonian stakeholders made a bid on the technology continuously creating the right conditions for everyone to use it. The trust came along as a collateral.

So even when the already mentioned incident with the eID card chips happened, it became clear that trust towards eID has not decreased. Furthermore, the overall usage of eID increased onwards. For the experts it is hard to decide what exactly led to this kind of response from the general public, but they do name: i) transparency and accountability when the incident was announced and explained to the population; ii) ownership and assurance of crisis solving; iii) availability of alternative eID options. Of course, some of the experts replied that citizens simply did not care or notice. The detected vulnerability and actions that fixed it afterwards have not affected their daily life and required on average little to zero effort from their side to make sure their identity documents are updated and, hence, remain valid. Yet, it should be said that in terms of trust this incident did not vanish away without leaving any damage. The CEO of the Estonian Certification Authority points out the following implication:

> *"I think that the biggest loss you can see that there was a lot of trust lost is if you look at the court cases that PBGB and Gemalto had after that. There was a company who had worked with the Estonian government for 15+ years; with every kind of real connections, and the good cooperation so far; and immediately, after the event, there was no goodwill left anywhere."*

5.4.2 Theme: Public Acceptance and eID Pervasiveness

This theme holds evidence in the form attributes that demonstrate and prove acceptance among the population. The parts of the discussions with the interviewed experts and their arguments that were selected for this theme and its codes reflect on several aspects which are the history and timeline of the deployment of eID, country specific attributes that contribute to acceptance, and the acquired reliance on eID, or in other words, dependencies. Figure 12 shows the codes of the given theme.

In broad terms, all experts agree that the eID public acceptance is very high in Estonia. Moreover, it is no less important than the technology itself. The Estonian CTO comments:

> *"So, from strategic point of view, public acceptance is absolutely critical. But the public acceptance cannot come before the solution itself."*

But as he states, public acceptance is not something that appears by default right after the technology is launched. Here, it is important to keep in mind a series of actions taken by the stakeholders throughout the years that resulted in the current state of the solution. More on this will be elaborated in the theme of "Actions and decisions".

In order to understand the degree of eID pervasiveness, a number of questions concerning user groups and their reliance on eID were asked.

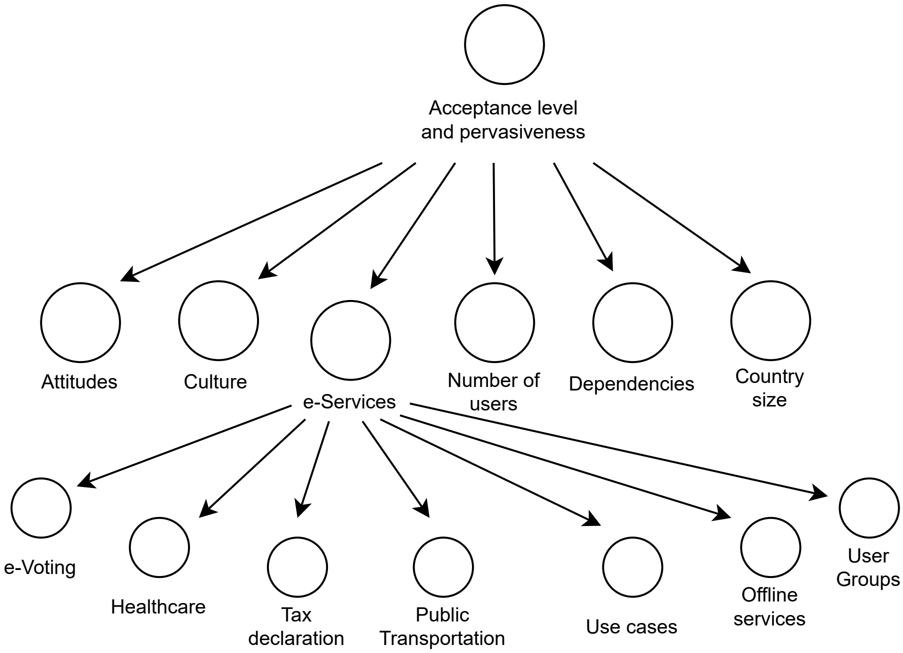


Figure 12: Theme "Public acceptance and eID pervasiveness".

When asked whether there are some user groups that could be perceived as primary ones who are more reliant on eID, the experts either disagreed with the idea of prioritizing some users over others, or explained the relativity of such prioritization. For instance, indeed, critical services like health care rely on eID continuing functioning since human life may depend on it, yet there are not enough grounds to lower the importance of other services. If one takes into account the amount of transactions in financial sector, then the banks can also be considered as primary users. The experts are reluctant to differentiate them according to importance. Without hesitance, two of them argued that each user is of priority in terms of service provision.

The aspect of dependency is different from the importance. Some user groups rely on the continuation of the eID enabled services. This is where the experts again named the sectors of healthcare and finance. Once the experts were presented a theoretical scenario of eID being compromised and they were asked to assume who would suffer first, the two named sectors were the first to be among others.

The experts who wished to remain anonymous mentioned the entrepreneurs:

> *"I just cannot exclude the people who work in business and the businesses. Because if your eID is not valid or not in use, or your certificates have been revoked, in that case, it means you are not able to do anything."*

He then continues his thought:

> *"Those at work or the most critical group, and I think it includes quite many citizens. For some citizens who do not need to use their ID in the work, I think, it's much easier, it is not stressed about it, it is something they use occasionally. But it doesn't have to be used even weekly, necessarily, depending on what they do. I think it's mostly work-related. And if you have any obligations, if it is something which comes from*

> *legislation, you as a citizen, if you have to perform some duties, and if they require eID for that, well, it's hard to say, it depends so much on the person. But quite often, you might face these situations daily or weekly when you have to use the eID for something."*

A major role plays the digital signature. The acceptance of this particular functionality of eID has grown over the years and is now widely used. As the Estonian CTO explains:

> *"[. . .] the way eID has been done, is that you can sign your documents, you can encrypt your documents, even if you don't have internet. As long as you have the software on the computer, and as long as your ID card is valid, I think this is really, really great. So not having the central dependency really works."*

At the same time, some other experts estimate that the reliance on digital signing is huge as it has become a part of software architecture and processes. More on this will be elaborated in the theme "eID concept".

Overall, the interviewed experts agreed that there is no way back in the sense of digitalization and electronic identity. While from a legal perspective a person is not depended on the eID and can (still) carry on with her life without getting involved into digital affairs, however, practically – it is not that easy anymore. As experts explained, yes, there are still people who have not used the "e-"part of their eID, that number is lower and lower. The usage of eID naturally varies: some use it extensively on a daily basis, and others use albeit rarer; however, at least one time per year one transaction is done by the heavy majority of the Estonian citizens – be it submitting a tax return declaration or paying bills. If a person does not want or know how to use public services online, service points and bureaus are available, though their number has significantly decreased over the years, as one of the experts from RIA mentioned. The other interviewee representing RIA has put in the following words:

> *"[. . .] people are kind of, let's say economically forced to use eID"*

The anonymous interviewee also commented:

> *[. . .] I would describe it that everyone who has any obligation to use the ID it might be it's just an individual citizen, it might be someone working on having certain responsibilities coming from the legislation, or it might be entrepreneurs. It might be people in business or public administration. Well, I think anyone is involved in a similar way."*

In order to understand better the situation with the dependencies in the user group of citizens, the experts were asked to explain if, who, and why are dependent on and more acceptable of eID.

In their responses, the experts did not cover all possible user groups but the most spoken of were the already mentioned entrepreneurs, the elderly, and the underaged. These user sub-groups certainly differ in their acceptance level, attitudes and reliance on eID.

The elderly and the underaged from the service provision point of view have always required special attention, approach, and inclusion. The experts' opinion is that these two groups are less reliant on eID but what is essential here is to ensure that everything is done to get them on board. The importance of raising awareness was emphasized. Again, the projects related to the increase of digital literacy and the e-ticket were brought up by the experts as effective measures to involve elderly. Additionally, the attention was brought to the fact that elderly require external help in learning about the digital world and its tools. Simple guidance and support of close ones is as helpful (if not more) as public campaigns and projects are.

As for the underaged, the interviewees believe it is much easier. Children who are being raised in the time of digitalization are more acceptable of online way of life including the affairs related to public services. Once they reach 16 years, they get their document and already the first transactions can be initiated. As the expert of RIA noted, a big part of children is issued their documents before 16 for traveling purposes. For this age group, the perspective of using paper-based services will never be an acceptable option. They may not be using eID over that period of their time, but it is guaranteed that acceptance level will be high onwards. Here is what the Estonian CTO says with regards to youth:

> *"[. . .] if the kids of today become older, start using these digital tools and don't know the life without them, then this will also boost these numbers, for two reasons. For one, they are themselves using it, more likely than people five or 10 years before, but at the same time, they are also going to make the older generation use them more; if a child graduates and becomes 18+ and start using their digital identity to do their own banking, then maybe, they're also going to make changes that their parents that might not use their digital identity enough, that maybe they would start using it more."*

Most of the interviewed experts have mentioned the country size as one of the factors that favored the high acceptance of eID in Estonia.

The CEO of the Estonian Certification Authority compared Estonia to Iceland size-wise and hypothesized in this regard the following:

> *"If I would compare our way of interacting that Iceland does it even better, because they have an even smaller community and there is no way to go from that island there. You cannot do anything that you are ashamed of; you cannot trick your fellow citizen there. Because you'll found tomorrow, there is no way to hide. That's what the small communities do: they put the responsibility on you."*

The experts also highlighted that the small size of the country also makes it easier to handle the bureaucracy. In other words, issuing a bit more than one million of eID cards is not comparable to those country cases where there are millions and millions more users.

During the discussion about the country size and other states in general, the subject replicability emerged. The Estonian CTO believes that many big countries that tried to roll out electronic identity failed as a result of attempting to do everything at once. The CEO of the Estonian Certification Authority also maintained the same position on replicability of eID in large countries. An expert from RIA also stresses that for large countries more time is needed. In Estonia, as he said, there is more transparency, and it is easier to reach people. It took twenty years to reach the current state of affairs, while in other countries, with bigger bureaucracy apparatuses that need to be rebuilt, it would take much longer than twenty years.

5.4.2.1 Attitudes and Culture The aspects of culture and attitudes have been noticeable parts of the discussion with the experts during the interviews.

While in previous rounds of research, the citizens were asked about eID and how often they need it and use it, the same question was addressed to the experts since most of them are representing the direct service providers of eID. Most of them replied that people, again, don't care much. But then CEO of the Estonian Certification continues that the indifference ends on a point when the solution stops working. Otherwise on a daily basis the citizens will not show their interest or even realize its importance.

Then, to explain why this interest is implicit, the CEO of the Estonian Certification Authority made the following comparison to illustrate the importance of eID to citizens:

> *"[...] if you would ask from the person next to you how important this is Circle K gas station that you see here. And they will say that doesn't matter. There is a next one behind the corner. But if you would ask how important is the fact that gas stations exist anywhere in Estonia? That's a different question. So I think that the working infrastructure, in general, also for the citizens is really important. But their own specific small eID is not because they kind of perceive that this is something that I can take the next one tomorrow as long as it works."*

One of the experts from RIA also maintained the same argument about indifference of people. As he explained, citizens want to spend as little time dealing with government as possible, and when they have to, these interactions have to, even if they happen online, take as less effort as possible. Hence, as he further continued, one of the most effective steps was to combine the eID with a service that would be both crucial and of high interest to all citizens. It was banking. Enabling banking with eID was the most effective "anchor" for the citizens, as the experts agreed unanimously.

> *"So if you give them a tool they can use for the e-banking, guess what happens? They start to like it."*

Surely, other services have also strengthened the acceptance, and more on this will be written below, however, it makes sense to continue on the current code description.

A cultural attribute or a cultural setting can have a range of impact on the public acceptance. Such concepts as "vision", "logic", "way of thinking", "mindset" were used to describe this sort of impact. The experts made several curios assumptions. One of them involved the possibility of historical outcomes and circumstances leading to modern order of things. The Estonia CTO commented:

> *"I do think that there's a cultural acceptance for failure that is more akin to this part of the world, and then perhaps some other countries... I suppose that this nation of Internet's people so to speak, we are more accustomed to things sometimes breaking, but we know that, you know, these things are going to work out well... Any country that tries to start doing eID, thinking that it's going to be perfect, he's already stepping off the wrong train at the wrong time. This is not going to work. I think that it's very, very important to be more ready for this kind of failure. So once you accept this, then it's going to be definitely much, much easier."*

The expert from RIA elaborated on the "philosophy", as he put it, that is used in Estonia that has led to the given order of things. According to him, the offline and online worlds are not separated. In fact, the virtual world is not a copy of the real world. It is actually a real world but just a different medium. Citizens as well do not make a difference between these two dimensions. It is one of the simple and clear truths, as he explains. To give an example, he takes the equal value that a paper document and an electronic document have. Then, another way to demonstrate the way of thinking among Estonian citizens, is to imagine a situation where a public affair needs to be taken care of, and if in other countries a person would first ask where he needs to go in order to do so, the very first thing a person from Estonia asks is which website he needs to open for that.

> *"[...] people have been mentally changed so much. So it's an assumption that everything is online. And when you see Estonians travelling and going somewhere and something happens, so they need to be in contact with authorities. And then they ask, you don't have any app for that or something? Do I need to go somewhere? What are you talking about?"*

The eGA founder also mentioned that technology was a priority from the very beginning – in early 1990s. It became prestigious to use it. The Estonian CTO mentioned that people have accustomed to technologies and innovations relatively early which allows now for an accelerated pace of mastering new and updated tech solutions.

> *"I think it's about the gradual shift of culture, to be more technology-minded, and to be more open for new things."*

> *"At the same time, we do think that Estonian citizen as such; they're willing to experiment a little bit more, I think this has been a success factor"*

5.4.2.2 e-Services The part of discussion that touched the subject of e-services reveals their role in the acceptance of eID.

One of the main take-aways is to realize that when eID is introduced, there should be services in place that can be accessed with this eID. The anonymous expert believes this to be another part of the country's success:

> *"It's about this overall approach of Estonia to enable the use of eID by introducing services in which it can be widely used. So I don't think that the decision for eID could be made alone or should not be made alone. If a country is to introduce an eID, it has to have a plan of introducing the services at once. It has to start immediately so that the citizens really have use for the ID."*

Another important take-away is to realize that eID will enable the use of services and the latter will be in demand if they are good. The experts unanimously agreed that the main indicator of a service is, first of all, whether people use it.

Of course, it can also be the case that a service is available and it is used, however, the process is not easy or convenient for the citizen. Therefore, a user-centric approach is required to make the services easy, intuitive, fast, convenient and effortless. A user-centric approach implies that the service provider understands the user. For that, as experts explained, use cases are crucial. One of the experts from RIA underlines the importance of use cases:

> *"[...] for government, it's really important that we need to have a solution that covers as much as possible, if not all of the use cases."*

He then continues with describing numerous daily situations where the citizen turns to government institutions pursuing a public service. In order to start the process of service provision, there is one common requirement: the eID. A person needs to be identified first. The provided document and its data need to be found in the governmental databases to see if both data match so that the service agent can proceed with the initial service request. Same situation applies online. The person needs to authenticate himself. For example, one of the use cases brought up by the expert from RIA is when a 16 years old child would like to receive a driver's license. He can either come to the bureau in person or visit the website. In both cases, eID is required. Or if a person wants to travel, he requires a passport. To get a passport, the person has to apply for it – with an eID.

> *"This ID card is like a mother of all identity documents; all other identity documents are based kind of on that. So, the same thing happens actually in private sector even before this ID card that if you want to have a membership or loyalty card, whatever; or you want to have a bank card or; you cannot get one if you haven't provided government issued document"*

The founder of eGA has also discusses the importance of use cases based on his personal experience. During a secondment trip, back in the early 2000s, he receives a call related to another work matter which requires a response in a form of signing certain documents. Even though, being en route to a different city, the work matter is resolved thanks to the Mobile ID that allows to receive the documents via Internet and use a website as a middle party to sign the documents by simply entering PIN 2 on a cell phone.

The essence of the use cases is to forecast as many events or situations where the solution can be applied in the most convenient way in order to fulfil users' needs. The more use cases there are, the more the solution will be kept being used reinforcing itself by the positive outcome and value it brings to the users. Therefore, a sufficient amount of services is crucial.

> *"[. . .] if you get a tool to access governmental services, and you can use it only once a year to declare taxes, of course, you're not interested. Even if you have this tool, after one year, you forget how to use it. . . we understood that we need to have some attractive services that people will be more than happy to use with this card. We needed to have something that people can use every day. So you don't forget how to use it."*

When discussing the use cases, the matter of eIDAS was brought into context. While EU member states are working towards cross-border interoperability and services, and there many available already, the experts point out that there are almost no use cases [II]. In other words, there are not many situations where an end-user can find a service enabled by eIDAS useful. Theoretically, we can assume such use cases, but as the RIA expert explained, the whole setting of cross-border services is in its preliminary stage. The stakeholders should start from a point of determining the needs of end-users and ensuring that the solution can fulfil those and be useful.

Several particular e-services were brought up during the interviews as the most effective in regard of introductory services that acquire end-users and create a basis for others and the overall awareness about the concept of e-service and what is needed to access it. It was already emphasized a few times that banking is the most heavily used service. All experts indicate , it has contributed to the public acceptance the most.

Then the turn comes to the healthcare services. These are indicated as the key services that have to be maintained. The access to medical records is crucial, especially during emergencies. This also applies to e-prescriptions. When the issue of dependencies was raised, and imagining that an eID crisis would affect the healthcare sector, the implications would be dire because of the high priority of delivering the services immediately on demand. The CEO of the Estonian CA commented on this:

> *"[. . .] those health records at disposal of doctors and they rely on access to the health information about the patient's normally on this kind of a strong electronic identity. Basically the whole health care would also be very, very quickly impacted. So like immediate lockdown there as well."*

In addition to multiple projects and campaigns related to new e-services that were launched in order to bring new users, it was important to keep both delivery channels:

online and offline. To make sure that users lean towards the online option had to be presented as more attractive and advantageous. One of the experts from RIA gave an example:

> *"I think the very important was like a soft motivation package provided by the tax declaration authority. If you declare the taxes online, you can get your refund within one week. If you declare taxes on the paper, you had to wait three months. What would your choice be?."*

The other expert from RIA added another point to the above one:

> *"[. . .] even if we have the services that are available as offline services, or at the service point, it's really uncomfortable, you need to travel somewhere, you need to stay in queue, and you have to pay more. So people are kind of like seeing it not as an option anymore and say no, no, no, no way I will go anywhere, or no way I will pay like a three times or double even double price for fee for that, never ever, I will do it online."*

5.4.2.3 Number of Users: Adoption Time and Number of Transactions The matter of e-services and use cases is tightly related to another small but not less important code family "Number of users" which then divides into two sub-codes: Adoption time and Number of transactions. The essence of these boils down to the growth of number of users over time as they discover and adopt services and solutions.

Here, we can look at all actions the stakeholders take to increase the usage of eID as "boosters". Since a national eID is a large-scale initiative, the required amount of such boosting actions can and has to be very high. To remind of an example, we can recall the words of the CTO of Estonia who reflects on the user uptake of Mobile ID when it was launched and how big of a difference it made to the overall use of eID if one refers to those years' stats.

The expert from RIA provides a detailed overview and breakdown of usage. He first refers to banking as one of the major boosters during the launch of eID card. He recalls:

> *"[. . .] in the first days already, like two major banks were accepting ID card and some enthusiastic customers started to use it. It took two-three years when we started to see the real growth of ID cards usage in the banking industry, also in the government, public sector industry. And somewhere after seven years, we got it saturated. By "saturated" I mean that we got the optimum of usage; took five to seven years, this grace time. And what I mean by optimum is that we have roughly 1.3 million inhabitants in Estonia, and we have 1.3 million cards in circulation, active cards."*

He then refers to 2011-2012 once the coverage reached almost entire population:

> *"[. . .] but I think it was almost 600,000 people who are at least once in a six month or something, and, or it was 700,000 people I don't remember exactly. And then we have like a once in three months was nearly 605,000. And every month monthly, we have around 500,000. And then then every week, there is like a 250,000-300,000 people were using this card. So if you look at these statistics, and if you look at the monthly statistics, then you understand that, basically almost in every household, that with the numbers, you can speculate, it's not the truth, but you can speculated that we have at least one person in every family who is using the eID once a month, usually pay the bills. But of course, we have people who are using more frequently. And then we have groups who are not using"*

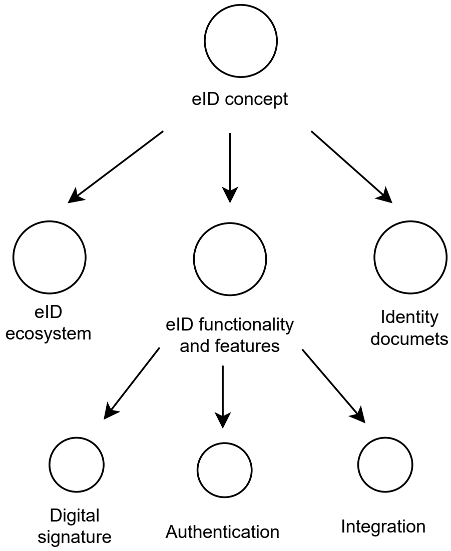


Figure 13: Theme "eID concept".

To complete and wrap up this breakdown of usage, he reminds about the numbers that come from the rest of eIDs, i.e., Mobile ID and Smart ID.

The anonymous expert argues that the adoption must take some time implying that a steady growth can be more advantageous, and numbers don't have to be an ultimate goal but rather the value delivered that creates a positive experience and encourages users to come back. This brings us back again to the concept of saturation mentioned by one of the experts from RIA. The saturation is strongly linked to the recurring use of solutions over time which in turn impacts the growth of numbers of unique users.

5.4.3 Theme: eID Concept

This theme formed itself the conceptual model of the Estonian eID. It brings together codes that represent various parts of the eID ecosystem and the technical infrastructure. It explains the importance of the idea behind the given conceptual model and how it determined the overall development path of eID in the country. Figure 13 shows the codes of this theme.

There are several crucial decisions or setups that presumably led to today's level of acceptance.

eID as a mandatory identity document In Estonia, owning an eID card as an identity document is legally mandatory. Each citizen, either from birth, or starting from the age of sixteen, must receive an eID card that contains a chip with unique data about the holder. The unique identifier contained in the chip is recorded in the population registry from the moment of birth registration. This aspect has been widely acknowledged as one of the main success factors when introducing national identity systems.

Having asked the interviewees what these factors are, they primarily name the this particular one among others. The director of eGA argues:

> *"ID card was compulsory document and [. . .] this has been one of the key enablers for e-government success also in Estonia"*

The anonymous expert also confirms that the card being mandatory is one of determining factors of acceptance. Having no alternative but just having the card worked out well, as he says.

The expert from RIA replies similarly:

> *"We didn't ask people "Do you want it? Do you want to have a chip on your card?" And we also didn't let the people decide if they want to activate or not keep it inactive; we decided that all cars have chip, there is no exclusion, and all chips are automatically enabled..."*

Most of the interviewed experts mention the term "concept" when asked about the success factor of eID public acceptance. They explain it as a conceptual model of eID that has to consist not just of an advanced technical solution but legal, organizational, and user aspects must be included. The Director of eGA emphasizes on the importance of having the concept of eID in place from the very beginning multiple times. He adds that if the concept is there, the state eventually saves significant costs. The CEO of the Estonian CA also points out the concept of eID and compares Estonia with other European states that although have identification, it does not exist as a part of a national IT infrastructure.

The founder of eGA names four components that create this concept: i) data itself; ii) interoperability iii) eID; iv) digital signature. More context is provided in Chapter 4. One of the experts from RIA explains the concept as an idea or a systematic approach to the eID implementation, its functionalities, and how it is going to facilitate access to services.

Additionally, it is worth to mention that eID being a mandatory identity document is also a part of its concept.

The Estonian eID is used for identification, authentication, digital signing, and encryption in different fields. The CEO of the Estonian CA mentions:

> *"[. . .] this cornerstone of Estonian government and services, is the identity that is common throughout different systems, both private and public."*

The director of eGA gives a similar statement marking that in some large countries, each sector issues its separate identity, e.g., governments, banks, enterprises, etc. However, he points out that such solutions would not have been viable in a small state like Estonia.

The expert from RIA mentions another interesting point on a single solution aspect:

> *"What in our philosophy, or in Estonia - we're trying to make, a virtual world is not even not a copy of real world. It's actually real world, but just different medium. So this is what we see that okay, if you accept the government documents, physical world, you should accept them online as well."*

Starting from the beginning, security has been a priority when designing the eID system, which is why the stakeholders made a bid on strong identity with complex cryptographic algorithms guarding personal data and its exchange. The expert from RIA states:

> *"[. . .] we have decided in Estonia that the government has to give a solution that works everywhere, it means that it has to have a highest level of assurance and technical security. That's the key. Because if you have the highest level, you can enter the low-level requirement, the systems that require low level, you can enter the system that require the substantial or this mid-level, or you can access also the high level."*

The anonymous expert as a foreigner who works in an Estonian organization provides his opinion on the Estonian setup:

> *"So how I look into it as a citizen and as an employee in an Estonian organization is that I see that the eID concept in Estonia was built by following the highest principles and going as high as possible in the safety and security of the system."*

The CTO of Estonia argues on the same point of prioritizing security of transactions:

> *"[. . .] you cannot really do bank transfers or notarized stuff with anything less secure than your eID."*

Having already indicated several times, eID and service are coupled together and have to exist side-by-side. This is a vital part of a successful national eID.

Experts also highlight the availability of the background algorithms as an open-source code that can be applied by anyone in the country for integration with their own services, be it a government agency or a private company. The CEO of the Estonian CA states that all the developments and components were made available to everyone, precisely:

> *"[. . .] the creation of supporting infrastructure, digital signature, creation software, the drivers for the ID card even came from us, the software to manipulate with a card or to change your PIN-codes. . . The drivers for the developers so that they could build their own solutions, basically, we open-sourced everything we do. . . "*

For instance, the CTO of Estonia reminds about TARA, an authentication software provided by RIA which enables authentication with national eID both within Estonia and other EU states:

> *"We do provide TARA for private sector as well, because it's an open source code. So private sector can take it from the Estonian code repository, and then start using it. And then they can essentially rely upon the ID as a whole, but they still need to set it up themselves."*

Here, it is a good time and place to refer to X-Road that is a part of the eID ecosystem, another pillar of the state digital government and its infrastructure which altogether facilitates a secure data exchange among all involved parties. It can be concluded from the experts' statements that the data exchange component is pretty much irreplaceable in the context of Estonia's digital government akin to the couple of eID and e-services – useless without one another. The centrally managed distributed data exchange layer was developed alongside eID together with e-services and various information systems that one by one were connected to X-Road over the years.

The abovementioned open-sourced code available to any service provider enables numerous kinds of integrations. The eGA director confirms these integrations are one of the instruments for increasing public acceptance:

> *"[. . .] most of those web-service providers are already integrated in the same platforms, eID possibilities, and it may be becoming not so critical problem for organisations to implement it in technical sense. So it should be simply supported and encouraged."*

The founder if eGA also reminds that ID cards can be used instead of loyalty and client cards for commercial purposes. Another major example of an eID integration into non-governmental processes is document management systems which are used in a multitude of organizations. As dealing with documents may require a long chain of actions such as acknowledgement, approval, and signing, the functionality of authentication and digital signing simplifies, optimizes and accelerates these processes and workflows.

During the interviews, the experts were asked whether given ad hoc electronic workflows increase eID public acceptance. The CEO of the Estonian CA, though, noted that this has happened since the technology was, again, open-sources:

> *"[...] the part that is important there, is really the, or at least was in history, that we have created a free of charge possibility to any small company to start digital document management. This has definitely improved the acceptance in the sense that none of those companies would ever digitalize their workflows on any other platform than email. So they will never invest anything into anything like that then... Yeah, I think that "yes" is the assumption that it was made available free of charge. I'm not sure that they would ever pay for that."*

The CTO of Estonia agrees such integrations should be benefited from:

> *"I think, yes. Because doing your own authentication and doing your own identity management systems are... well, you still need to do identity management... but technically, doing your own authentication is sort of reinventing the wheel."*

Yet, he considers that it is not about document management facilitation with eID per se, but the key is the session itself. He then again brings up TARA:

> *"I think that the good example here is the TARA that we are using in Estonia, rather the setup area, which is a sort of gateway to authenticate and log in your users. So you essentially authenticate user, and then you trust the authentication. You trust that the session is valid for this specific user, and then it can use it in your document management systems or elsewhere. So I think that this by itself strengthened the eID acceptance, that you're using sessions, because sessions were used already before the eID."*

5.4.4 Theme: Actions and Decisions

This theme holds evidence on the stakeholders' actions with respect to eID implementation and the systematic efforts in a form of various partnerships, policies and requirements. The codes of this theme are shown on Figure 14. This theme presents itself as an excellent case of institutional design analysis perspective as it precisely demonstrates three types of design are interrelated among each other and function in a form of a design process. This will be discussed in Chapter 6.

It is worth noting that statements presented in this final theme overlap with the already described statements above. The topics of eID, e-services, data exchange are raised in this part. What is different is the angle. While previously abstract features and attributes, technical components, and circumstances were the main subjects, this theme focuses on the results of cooperation between the stakeholders of the Estonian identity management and implications for the eID public acceptance.

5.4.4.1 Service Providers: Actor Constellation Cooperation of stakeholders in the beginning of 2000s is widely considered as one of the crucial factors of the digital government's success. Some argue it is the size of the country that hence makes the communication and decision-making easier; some say it is the willingness of the parties to work together; others point out the choice of moving in the direction of IT. The eGA founder says the following with regards to the third arguments:

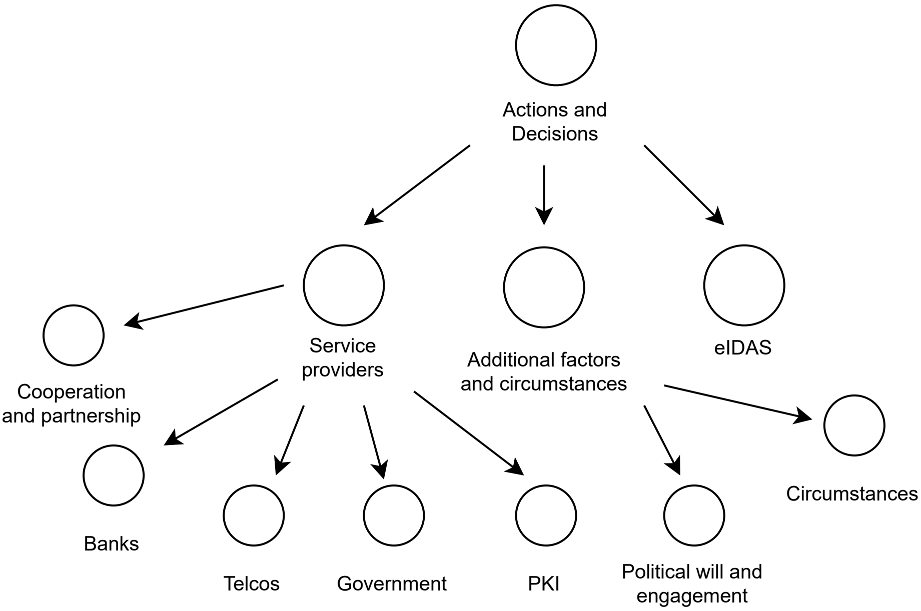

Actions and Decisions
Service providers
Additional factors and circumstances
eIDAS
Cooperation and partnership
Banks
Telcos
Government
PKI
Political will and engagement
Circumstances

Figure 14: Theme "Actions and decisions".

> *"[...] we tried to find some magic way and we attributed this magic to technology."*

One of the experts of RIA provides a retrospect into the chain of events and decisions that led to the current state of affairs. The government decided to cooperate with the Bank Association which resulted in the establishment of a Certification Authority as a private entity that began issuing certificates for all types of ID and signature means. The CA was created by two major Estonian banks whose clients represented the 70% of the country's population. The third founder was a state-owned telecommunication company. Already in the 1990s, the e-banking began to develop, and meanwhile, the state already had plans to start issuing new identity documents. The common interest of both public and private sectors in creating a Certification Authority was trust and security. Back then, as the expert from RIA puts it, there was no eIDAS or European Union who would provide some common framework that would cover and regulate web security. Therefore:

> *"[...] it was like a win-win concept - we both need it, let's cooperate on that and create together. But the beautiful thing with that was that from the technical perspective, if you have a one certification body with a one root certificate that issues to two different actors, certificates, then automatically technical trust is created, because they're using from the same root coming certificates. And therefore, it was no technical issue for the banks to start to accept government-issued eID. Because technically, all the pre-assumptions were already made... and it was a good cooperation."*

The CEO of the Estonian CA states:

> *"[...] in Estonia, the electronic identity was brought out in a way where this launch was coordinated and agreed by the private sector and public sector; and banks very much supported in the public messaging."*

Overall, the experts agree that there was a strong political will and engagement coming both from the public and private sector. Firstly, as the eGA director mentiones, the empowerment existed even in a legislative level. The laws were in a way promoting the technical infrastructure developments such as eID, X-Road, and conducting digitalization of the public sector in general. The CTO of Estonia believes that willingness of stakeholders to move forward with these developments is as much important as having the resources to execute that. He says:

> *"I definitely believe that it's not possible to do it without political investment, not just in money, but investment in thought and vision. I think it's absolutely critical. So I don't think these things can happen without this kind of investment, at least in terms of e-government. It is absolutely critical. You cannot do it in a grassroot manner. It just will not work well enough. You need to have invested agents."*

The anonymous expert acknowledges the political will to have brought positive outcomes:

> *"It's about the political decisions, which sometimes have to be actually quite restrictive decisions, too, because I don't believe that e-governance can be built in any other ways, but making the high-level decisions, which can be seen like, enforcing something to happen, it's really pushing the things, it's saying that, yes, this is how we do it here. And Estonia has been successful in it."*

The CEO of the Estonian CA also brings up the aspect of involving the right stakeholders that are capable of value creation and quality:

> *"Also, the telcos at the time, at least some of them had a very clear statement that the brand is connected to innovation. So they are bringing the innovation to the country. So I think that there were a lot of companies who were related to the image of technology, technologically advanced companies. And the services in the sense worked. So they actually provided something meaningful to the people. That meant that it wasn't just a big part of why we do innovative things, but it actually paid off on a daily basis. So that's, I think, where the trust came from."*

5.4.4.2 Circumstances Interestingly, during the discussion with one of the experts, the government CTO, the topic of replicability of Estonian eID was touched, and then the expert was asked whether it were the right circumstances that to some extent determined the development path of e-government in the country. Here is what the CTO replied:

> *"I think that it is perfectly correct to say that a lot of ducks were in the row or the plants were aligned perfectly for Estonian digitalization success to happen the way it did, and especially on the foundation of eID. But I would also say that, you know, I think it can be replicated, if the intent is there, and if the desire is there, and the will is there."*

He describes the circumstances as perfect conditions:

> *"[. . .] ideal sort of environment where it happened that we had regained our independence. And then as we had regained our independence, we had this sort of a wild west type of regulatory world that we needed to build up at the time when digitalization was becoming a thing and computers and internet were becoming a thing."*

Then he continues:

> *"This is perfectly true, this is hard to replicate, these kinds of situations in another country. But at the same time, the reason why we're talking about this today, or the reason why you are doing this kind of research is because Estonia was small enough where we could do it nationwide. And at the same time, we were big enough for it to matter to other countries and other researchers and other participants. And this place is us in this unique position."*

However, he says afterwards the following:

> *"[...] it would be somewhat a misstep to assume that just because Estonia had this perfect environment for this to flourish, that it cannot be done in other countries."*

The government CTO is certain that the Estonian experience with eID is scalable. He cautions though that one should not be eager to scale the eID right away to a national level and expect it to succeed. The key is to start small:

> *"I think that it would be easily possible to do it regionally. Maybe in a within a state, maybe within a county."*

He concludes his thoughts on the subject of lucky circumstances by circling back to the public acceptance:

> *"[...] we didn't really have success, before the public accepted this new plastic card and digital identity by having an actual real-life appliance for it. It doesn't happen, you know, before that you just can't, you know, send everybody the tools and then say, you know, do something with it, stuff will happen."*

The CEO of the Estonian CA and one of the experts of RIA also mentioned the coincidents and circumstances to have been favourable.

The CEO of the Estonian CA believes that any kind of this large-scale project involves a certain degree of luck. The expert from RIA tells that it was a lucky situation that while planning to introduce an eID, it became easier to do so since an identity document reform was going to be adopted at that time anyway.

This concludes the third data collection and research round. The interviews have provided a great deal of insights: some completely new, some of them repeating, some of those that confirm the previous findings, and some that contradict with what is already known.

The experts unanimously agree on the importance of the public acceptance of eID and its big role in the success of an e-government. They have named numerous aspects, facts, events and circumstances that determined the outcome story of the Estonian eID. It is a challenge to measure which of those have been certainly the most impactful, but naming a few, it would be: i) taking the action early, ii) prioritizing IT, iii) cooperating with private sector and its innovative representatives, iv) integrating eID with financial sector, v) creating meaningful services, vi) providing them to entire population, and many more.

Keeping in mind that it takes time and continuous effort for the solution to start working and get accepted, the experts seem to emphasize on consistency. This includes the general promotion of computers in the late 1990's and early 2000s, together with simultaneous creation of public services that oftentimes are supported and enabled by private companies and telcos (telecommunication companies).

What became clear after talking to the experts, that one cannot simply exclude a single fact or argument from the given case of the Estonian eID. Each and every of them have played its part, and the main goal of this round of research was to grasp the holistic picture and ensure nothing is overlooked. As the government CTO notes, many can benefit from this story and case of eID; none of them will probably be in the exact same position, but starting with a small and local project to scale it further is the way to go.

The overall implications and conclusions of the entire set of results obtained within this work will be discussed in Chapter 6.

6 Discussion

In this work, the aim has been to reveal the subject of eID public acceptance through the case study of Estonia. This chapter discusses the main findings from the conducted research rounds and the implications they may have.

The conducted case study research followed by the guidelines of Yin [139] consists of a single embedded case study. The embedded units of analysis are aligned with the research questions answered in this Chapter. The type of inquiry accommodated is mostly explanatory (excluding unit of analysis 1 which is partially exploratory; see Table 2.1). To provide meaningful and elaborated answers, qualitative data analysis techniques were used to generate in-depth explanations from the collected over the years realm of data.

Relying on the body of knowledge about technology acceptance and a number of theories, the inquiry was designed so in order to obtain specific pointers in a real-life case where part of the story is told by the end-users themselves. Therefore, to increase the validity of factors, they were firstly derived from the literature sources, but particularly those in which the outcomes were obtained on the basis of empirical studies of the end-users views. This has been the exploratory component within this unit of analysis.

The eID public acceptance factors identified as a result of SLR (see Section 5.2) were then tested and validated through the next research rounds.

The factors were incorporated in the citizens' questionnaires in the next study (see [IV,V]) and the in-depth expert interview questions. This allowed for their further validation through the received answers of respondents and through the conducted interviews.

The questionnaire's goal was to investigate Estonian citizens' perceptions of and attitudes towards eID. Given it is wide-known that eID is a mature and stable component of Estonian e-government, the research round employed an explanatory type of inquiry to obtain a detailed view and deep understanding of population's perspective of eID. There were several take-aways learned from this research round. A high level of trust towards eID and the service providers was confirmed. The opinion of the interviewed experts later confirmed and backed up this finding.

The respondents demonstrated satisfaction with the currently available authentication options. Considering the security concerns and recent events [36], [VI,VIII], the number of alternatives offered to end-users currently seems to be optimal and convenient. The discovered perceptions and attitudes of Estonian eID allow for further study of technology acceptance on an individual level.

The last research round, as a part of a third unit of analysis, also employed an explanatory inquiry to answer the RQ3 on the importance of eID public acceptance in the success of e-government.

The core argument is that the top experts from their fields agreed unanimously on the public acceptance being one of the key success factors of e-government in Estonia.

The thematic analysis of the interviews and the diverse code structure showed just how many variables are at play and how much each of them can have an impact on the overall outcome of the public acceptance.

Estonia introduced eID on the verge of a new history chapter after becoming independent Taking the path towards integration of emerging technologies into the public sector and using the help of private sector was undoubtedly a turning point for the state's future we observe today. The experts acknowledge the role banks and telecommunication companies have performed in the establishment of eID and e-services. It was relatively easy to do so considering the size of Estonia, as they put it. Each party showed commitment to a common goal and made a tangible contribution. At the beginning of the roll-out, the support from banks was invaluable considering the coverage of population who were their customers, and further on, as the new eID forms appeared, the telecommunication companies entered the scene. Integrating eID into financial services was a crucial step since, as during interviews experts mentioned, it created motivation for the end-users to try a new state-provided solution that is linked to something that is of high interest and value for the end-users – money. In this sense, banks served as a trust bridge between the end-users and the state. If it is assumed that citizens trust their money to the banks, and the banks in turn offer a solution that is claimed to be more secure and is available to anyone anyway, then another assumption is that perhaps banks must trust the state as the solution provider, and hence it is worth trying this solution. Obviously, it took several years until the ID cards were issued to all citizens, in terms of the DOI theory [103], this time period allowed for the "early adopters" to familiarize with the new solution and later on demonstrate its benefits and usefulness to "laggers". The role of "early adopters" and "opinion" leaders is also abundantly discussed by Palginõmm [56]. Nowadays, the extensive usage of eID as a day-to-day pervasive tool has become habitual [46]. This habit has also emerged to numerous use cases incorporated: be it a public official's account in electronic document management system, a citizen's PC with digital signing software he uses to sign a contract and then send it over email, or an e-commerce website that allows its customers log in using their ID card or a Smart ID account.

It can be assumed with a high level of confidence that the efforts of stakeholders invested into promotion and diffusion of eID reaped fruitful results. Apart from creating the actual technical infrastructure, eID, and e-services, the projects that were initiated for raising citizens' digital literacy and awareness of the e-service options shortly proved to be a great boost for the public acceptance. For the citizens it created a visibility of the state's interest in delivering public value. The fact of an opened public-private partnership added up to a positive image, transparency and trustworthiness of eID and e-services.

It is natural that once a solution becomes so heavily used, dependencies are very likely to occur. During the discussion with the interviewed experts, many of these were brought up. eID has been acknowledged as a part of the state's critical infrastructure [VI]. Security and privacy remains the highest priority when it comes to electronic identity which again brings us about the ROCA incident from 2017. It serves as a wake-up call to the identity providers and other stakeholders involved and reminds about constant awareness of risks which are always there [56]. Nevertheless, after the incident, the numbers of eID usage continued to increase. To a large extent, in experts' opinion, a policy of honesty about the incident was employed and clear action plan was articulated to the general public [VIII]. The given incident and its crisis management did not reflect on the citizens' perceptions of and attitudes towards eID. This concludes RQ2 with the arguments obtained from the last research round.

As a matter of fact, this is the place where eID and its public acceptance should be discussed in the context of a large-scale information system. eID is so much more than an albeit complex and extended amount of technical assets, but a system that also involves institutions, actors, games, and rules [136, 137, 64] and public acceptance is a part of it.

6.1 Institutional Design of Electronic Identity in Estonia

To extend the answer to the final research question, i.e., RQ3, let us recall the institutional design framework by Koppenjan and Groenewegen [64] that was brought up in Section 6 of this work. Bharosa et al., used it to interpret the Estonian e-government setting (see Table 11) [27]. We adapted the table by adding an interpretation of Estonian eID in the context of the institutional design to show its relevance to the current case study. This extension allows for an accessible and compact view of a national large-scale information system such as eID with its mapped assets, including public acceptance. Public acceptance performs a role of one of the crucial enablers of eID and hence e-government. The input for the eID context interpretation is taken from Chapter 4 and Section 5.4.

Layer 4: Informal institutional environment that reflect various norms, values, and culture are reflected in the interaction of stakeholders behind the national electronic identity management. Based on the many statements from the interviews conducted in the last data collection round (see Section 5.4), the tight cooperation between public and private sectors has been there along all the way of introducing eID. As the government CTO mentioned, both sides were invested and committed to a common goal. Moreover, trust that comes from the citizens, public's digital literacy, and political will are relevant within this layer.

Layer 3: Formal institutional environment is reflected in the legal arrangements in case of Estonia was settled from the beginning of identity document reform [95, 56]. It has been aligned with the rest of legislation that defines and mandates e-government- and eID-related components and their provisions.

Layer 2: Formal and informal institutional arrangements can be seen from the mutual recognition of stakeholders' roles, functions, and responsibilities. An example is the single certification authority of Estonia represented by a privately-owned company. While SK provides public key infrastructure related services to the state that in turn steers the national electronic identity management, the SK at the same time provides Smart ID as a service that is now recognized and accepted on a public-sector level. Then, the projects and initiatives aimed at raising citizens' awareness of eID also belong to Layer 2. Lastly, the Estonian eID itself can serve as an example, as it was launched as an outcome of a public-private partnership (see Chapter 4).

Layer 1: Actors and games are represented by the individual agencies, companies, and households that interact and have within themselves internal structures and hierarchies [64]. In the context e-government and eID, it is the service provision and related to it arrangements between and within institutions. For the end-user, whether it is an individual or a company (in Koppenjan and Groenewegen's terms, a *household*), the service is provided as an outcome of a set of processes, agreements, and resources coming from one or more organizations interacting with one another. In other words, once a citizen, for instance, intends to submit whatever kind of application via state portal, he uses a range of other services that are pre-set by actor, i.e., several service providers, and afterwards, are handled at least by one actor, i.e., the service provider.

These are only few examples of how a large-scale information system can be mapped by means of institutional design. In the context of this work, it proved to be helpful in clarifying the roles of stakeholders and their interactions from the perspective of eID public acceptance. The next step would be to create an extended and more comprehensive map of stakeholders, their assets, and arrangements among them within the entire eID ecosystem in the pursuit of "highly collaborative frameworks for seamless delivery towards citizens" [27].

While linking all findings of this work, one of the main insights is how holistic and interconnected they are. Especially, this became clear during the last round of data collection and research, when the experts shared their thoughts on the many assumptions made previously. Public acceptance is both a tool and a result. It is a phenomenon that emerges at some point along the way of a solution existing and being used, and later on can be leveraged for other purposes, e.g., introducing and reinforcing new services, use cases, and functionalities. This process reaches a point of perpetuity and hence the maturity of the system itself.

Table 11: Institutional design of Estonian e-government ecosystem (Source: adapted from [27]).

Layer	Context of e-Government	Context of eID
Layer 4: Informal institutional environment	Government is trusted [85], [VI] and consist of reliable institutions to meet performance expectations. Open interaction between public agencies and the private sector	National electronic Identity Management functions on the basis of cooperation between public agencies (RIA, PBGB, Ministry of Economic Affairs and Communications, etc.) and private sector (SK, banks and telcos). Trust, technology, political will
Layer 3: Formal institutional environment	Exhaustive set of stable legal assets that are designed with respect to (resp. co-designed with) the technological assets of the e-government ecosystem	Clear legislation on identity documents, digital signing, and PKI, that are compliant to eIDAS Regulation. eID is mandatory
Layer 2: Formal and informal institutional arrangements	Centralized steering of e-government. Whole-of-government approach to modernize service delivery in a joined-up manner. Strong focus on economies of scale: the use of state eID, national registries and X-Road for both public and private services. Focus on creating transparency by showing all transactions	Centralized national electronic identity management. Common acknowledgement and recognition of different eID options across sectors. Open-source technology. Public LDAP certificate directory. Digital format and digital signature preferred over physical ones.
Layer 1: Actors and games	Innovation by government for the entire society. Central government carries risks of innovation, strong emphasis on innovation and service delivery by government agencies. Experimentation by the government is stimulated and in this way knowledge and understanding of the public and technology is created	High priority of technology and innovation across entities. Strong emphasis on security and awareness with the initiative coming from both public institutions and private sectors. Tight cooperation, partnership, and support on a service provision level

To conclude, we would like note and remind the following about eID public acceptance. It is not a tangible and straightforward concept. As of now, it still cannot be precisely quantified, nor can we state that it is a final destination or a constant. Electronic identity technologies are not necessarily developed prioritizing user needs in convenience or usefulness. In most cases, it is security that is the priority. But the task of identity providers is to use the technology in a way so that it becomes a service that delivers value to the user and meets his needs to the fullest.

6.2 Limitations and Future Work

One of the concerns about the case study methodology is generalizability of the case study conclusions [139]. Since we are relying on the analytic generalization where the outcomes are generalized on a theoretical level and can be further applied in other case studies. Our goal was to acquire a deep understanding of the public acceptance phenomenon in Estonia with a focus on what it consists of, what actions of which stakeholders can cause it and affect it, and why is it important for a country. The context of Estonia provides a scene, and we did look into the peculiarities Estonia has (e.g., country size, history background, culture, etc.), but the forefront attention was paid to "how" the public acceptance built up and what was done by whom to achieve it. Hence, understanding the circumstances allows to choose and taylor strategies and approaches more effectively and with higher precision. And this is where the acquired theorized generalizations can be applied. If we come back to words of the Estonian government CTO (see Section 5), he states with high confidence that the case of Estonia bears plenty of lessons to learn from, but replication should be done in a scalable way which allows for more flexibility. This dissertation provides generalized directions and highlights on public acceptance of eID and how it can influenced.

Yin points out that case studies have been considered by many researchers as inherently subjective [139]. During the analysis of first, second, and third data collection rounds, the sample sizes examined were relatively small, but the quality of results were then validated through the analysis of the fourth data collection round. The thematic analysis showed that most of the assumptions and findings previously obtained, do match with experts' statements and opinions, and further elaborate them with additional insights and details.

To address these limitations, new studies in different settings using the current premises must be conducted. That way, the factors of eID public acceptance can serve as indicators and help critically assessing the electronic identity situation in a country or a region. Through such evaluation, the importance of public acceptance is then revealed pointing out to those areas where improvements are need to be introduced.

As the technology paces forward quickly, new developments are about to be introduced in many national electronic identity schemes, by means of obtained findings, public acceptance towards eID can be leveraged to smooth the process of adoption. During the interviews, the experts shared their thoughts on the necessity of evaluating risks to public acceptance of eID when introducing new features and functionalities. Their forecast is that in the near future biometric technologies will prevail on the market of electronic identity technologies. One of the endeavours is to use obtained findings with regards to acceptance factors and conduct studies in countries, where such technologies are already embedded in the national electronic identity schemes. An important aspect to be investigated here is the actors' constellation [68] and institutional design framework [64] to ensure a bird-eye view on the entire eID setting.

It is worth recalling eIDAS that was mentioned earlier in this dissertation and appeared as a code during thematic analysis, however, the subject was not described in detail. We suggest to examine eID public acceptance in the EU members' common endeavour to reach cross border interoperability as one of the directions for future work [II]. Additionally, a proposal to amend the eIDAS regulation [1] that revisits its scope, tools, and goals, widens the possibilities and focus points for the potential future work.

7 Conclusion

This work is the first comprehensive study on the aspect of public acceptance of eID. We provide a vast description of what eID public acceptance factors derived as a result of systematic literature review. The identified factors can be used in future research as benchmarks for examining and interpreting the public acceptance of eID in other countries. With additional research and cooperation with interested parties, potentially, these factors can be formalized and quantified.

This work is also the first scientific study on the user perspective of eID in Estonia. Considering the uneven ratio of research on different aspects of eID available, we provide an overview of user perspective by investigating how people in Estonia are accustomed to eID, how often they use it, and how favourable people are towards eID. Our findings are backed up with the statements and opinions of the top experts in the field of electronic identity who also confirm the vital role of eID in the success of e-government.

Hence, we generalize these results via the model of institutional design of Koppenjan and Groenewegen [64] and propose a bird-eye view on the niche of eID public acceptance in such large-scale information system as e-government.

eID public acceptance is both a journey and a destination. It does not come as a package deal when eID is introduced but requires a comprehensive approach in decision-making, communication among stakeholders, and, most importantly, focus and priority on the people who ought to use it. This work shows just how complex and important the phenomenon of eID public acceptance in fact is. The case of Estonia demonstrates how public acceptance has been building up and how much common effort it can take.

It has been now 20 years since the first ID cards where introduced and eID has been in use. During these two decades, Estonia outran most of the countries by becoming an advanced digital state with a strong electronic identity management. This work sheds light on one of the pillars of eID – the public acceptance.

List of Figures

List of Tables

References

[1] [last accessed 15/12/2021] https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation.

[2] [last accessed 24/11/2021] https://www.politsei.ee/en/instructions/digital-id.

[3] [last accessed 24/11/2021] https://www.politsei.ee/en/instructions/e-resident-s-digital-id.

[4] [last accessed 27/11/2021] https://e-estonia.com/solutions/.

[5] [last accessed 27/11/2021] https://pilet.ee/viipe/uhiskaart/persod/perso.

[6] Id4d practitioner‘ guide: Version 1.0. Technical report, World Bank, 2019.

[7] J. K. Adjei. *A Case for Implementation of Citizen Centric National Identity Management Systems: Crafting a Trusted National Identity Management Policy*. PhD thesis, Aalborg Universiy, 2013.

[8] S. Ahrenstedt, J. Huang, and L. Wollny. *A Study on Factors Influencing the Acceptance of Mobile Payment Applications in Sweden*. Jönköping International Business School, Jönköping University, May 2015. Bachelor Thesis in Business Administration.

[9] G. Aichholzer and S. Strauß. The austrian case: multi-card concept and the relationship between citizen id and social security cards. *Identity in the Information Society*, 3(1):65–85, 2010.

[10] P. Ajibade. Technology acceptance model limitations and criticisms: Exploring the practical applications and use in technology-related studies, mixed-method, and qualitative researches. *Library Philosophy and Practice*, 2018.

[11] I. Ajzen. The theory of planned behavior. organizational behavior and human decision processes. *Organizational Behavior and Human Decision Processes*, 50(2):179–211, 1991.

[12] O. Al-Hujran, M. Al-Dalahmeh, and A. Aloudat. The role of national culture on citizen adoption of egovernment services: An empirical study. *Electronic Journal of E-Government*, 9(2):93–106, 2011.

[13] S. Al Marzooqi, E. Al Nuaimi, and N. Al Qirim. e-Governance (G2C) in the public sector. In *Proceedings of ICC'17 – the 2nd International Conference on Internet of Things, Data and Cloud Computing*, pages 1–11. Association for Computing Machinery, 2017.

[14] A. Alkhalifah. *Factors Effecting User Adoption of Identity Management Systems: an Empirical Study*. PhD thesis, School of Information Systems, Technology and Management, The University of New South Wales, August 2013.

[15] A. Alkhalifah and S. Al Amro. Understanding the effect of privacy concerns on user adoption of identity management systems. *Journal of Computers*, 12(2):174–182, 2017.

[16] A. Alkhalifah and J. D'Ambra. Factors effecting user adoption of identity management systems: an empirical study. In *Proceedings of PACIS'2012 – the 16th Pacific Asia Conference on Information Systems*, page 182. AIS Electronic Library, 2012.

[17] A. Alkhalifah and D. John. The role of trust in the initial adoption of identity management systems. In H. Linger, J. Fisher, A. Barnden, M. L. Chris Barry, and C. Schneider, editors, *Proceedings of ISD'2012 – the 6xt International Conference on Information Systems Development*, pages 25–39. Springer, 2013.

[18] G. Allison and P. Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis, 2nd ed.* Longman, 1999.

[19] K. C. Andermatt and R. A. Göldi. Introducing an electronic identity: The co-design approach in the Canton of Schaffhausen. *Swiss Yearbook of Administrative Sciences*, 9:41–50, 2018.

[20] E. I. S. Authority. The information system authority will adopt smart-id for state services, Sep 2019.

[21] J. Backhouse and R. Halperin. A survey on eu citizens trust in id systems and authorities. the european e-identity conference. Technical report, Information Systems and Innovation Group, London School of Economics and Political Science, 2007.

[22] J. Backhouse and R. Halperin. Security and privacy perceptions of e-id: a grounded research. In *Proceedings of ECIS'2008 – the 16th European Conference on Information Systems*, pages 1382–1393. AIS Electronic Library, 2008.

[23] J. Backhouse and R. Halperin. Approaching interoperability for identity management systems. In K. Rannenberg, D. Royer, and A. Deuker, editors, *The Future of Identity in the Information Society*, pages 245–268. Springer, Berlin, Heidelberg, New York, 2009.

[24] D. Belanche, L. V. Casaló, and Flavián. Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption. *Cuadernos de Economia y Direccion de La Empresa*, 15(4):192–204, 2012.

[25] I. Benbasat. An analysis of research methodologies. In F. W. McFarlan, editor, *The Information Systems Research Challenge*, pages 47–85. Harvard Business School Press, Boston, Massachusetts, 1984.

[26] I. Benbasat, D. K. Goldstein, and M. Mead. The case research strategy in studies of information systems. *MIS Quarterly*, 11(3):369–386, 1987.

[27] N. Bharosa, S. Lips, and D. Draheim. Making e-government work: Learning from the Netherlands and Estonia. In S. Hofmann, C. Csáki, N. Edelmann, T. Lampoltshammer, U. Melin, P. Parycek, G. Schwabe, and E. Tambouris, editors, *Proceedings of ePart'2020 – the 12th IFIP WG 8.5 International Conference on Electronic Participation*, volume 12220 of *Lecture Notes in Computer Science*, pages 41–53. Springer International Publishing, 2020.

[28] B. Boguraev, C. Kennedy, and S. Brawer. An architecture for content analysis of documents and its use in information and knowledge management tasks. *ACM SIGCHI Bulletin*, 30:64–71, 1998.

[29] T. Bonoma. Case research in marketing: Opportunities, problems, and a process. *Journal of Marketing Research*, 22(2):199–208, May 1985.

[30] R. E. Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[31] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[32] V. Braun, V. Clarke, E. Boulton, L. Davey, and C. McEvoy. The online survey as a qualitative research tool. *International Journal of Social Research Methodology*, 16 Aug:1–14, 2020.

[33] J. Brewer and A. Hunter. *Multimethod research: A synthesis of styles*. Sage Publications, Inc, 1989.

[34] L. G. Brown. The strategic and tactical implications of convenience in consumer product marketing. *Journal of Consumer Marketing*, 6(3):13–19, 1989.

[35] J. Brugger, M. Fraefel, and R. Riedl. Raising acceptance of cross-border eid federation by value alignment. *Electronic Journal of E-Government*, 12(2):178–188, 2014.

[36] A. Buldas, M. Jung, K. Kuivjõgi, A.-M. Osula, R. Ottis, J. Priisalu, L. Tallinn, and T. Vaks. Id-kaardi kaasuse õppetunnid. Technical report, Tallinn University of Technology, 2018.

[37] P. D. Bush and M. R. Tool. Foundational concepts for institutionalist policy making. In *Institutional Analysis and Economic Policy*, pages 1–46. Springer, 2003.

[38] C. Cap and N. Maibaum. Digital identity and its implications for electronic government. In B. F. Schmid, K. Stanoevska-Slabeva, and V. Tschammer:, editors, *Proceedings of I3E'01 – 1st IFIP Conference on E-Commerce, E-Business, E-Government*, pages 803–816. Kluwer, 2001.

[39] F. Chandio, F. Burfat, A. Abro, and H. Naqvi. Citizens' acceptance and usage of electronic-government services: A conceptual model of trust and technological factors. *Sindh University Research Journal-SURJ (Science Series)*, 49(3):665–668, 2017.

[40] S. Chauhan and A. Kaushik. Evaluating citizen acceptance of unique identification number in india: an empirical study. *Electronic Government*, 12(3):223–242, 2016.

[41] J. W. Creswell. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 2nd edition*. SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, 2003.

[42] J. W. Creswell. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches, 3rd edition*. SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, 2007.

[43] C. Cuijpers and J. Schroers. eidas as guideline for the development of a pan european eid framework in futureid. In H. Hühnlein and D. Roßnagel, editors, *Open Identity Summit*, volume 2015 of *GI-Edition Lecture Notes in Informatics*, pages 23–38. Gesellschaft für Informatik e.V. (GI), 2014.

[44] F. Davis. *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. PhD thesis, Sloan School of Management, Massachusetts Institute of Technology, February 1986.

[45] F. D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3):319–339, 1989.

[46] G. H. S. M. de Moraes and F. de Souza Meirelles. User's perspective of eletronic government adoption in brazil. *Journal of technology management & innovation*, 12(2):1–9, 2017.

[47] D. Draheim. On architecture of e-government ecosystems: from e-services to e-participation:[iiwas'2020 keynote]. In *Proceedings of the 22nd International Conference on Information Integration and Web-based Applications & Services*, pages 3–10, 2020.

[48] Y. K. Dwivedi, N. P. Rana, H. Chen, and M. D. Williams. A meta-analysis of the unified theory of acceptance and use of technology (UTAUT). In M. Nüttgens, A. Gadatsch, K. Kautz, I. Schirmer, and N. Blinn, editors, *Proceedings of TDIT – the 8th IFIP International Working Conference on Governance and Sustainability in Information Systems: Managing the Transfer and Diffusion of IT*, pages 155–170, Berlin, Heidelberg, New York, 2011. Springer.

[49] M. Fishbein and I. Ajzen. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA, 1975.

[50] J. Goldstein, R. Angeletti, M. Holzbach, D. Konrad, M. Snijder, and P. Rotter. Large-scale biometrics deployment in europe: Identifying challenges and threats. *JRC Scientific and Technical Reports*, 2008.

[51] R. E. Goodin. *The theory of institutional design*. Cambridge University Press, Cambridge, UK, 1996.

[52] L. F. Goodstadt, R. Connolly, and F. Bannister. The Hong Kong e-identity card: Examining the reasons for its success when other cards continue to struggle. *Information Systems Management*, 32(1):72–80, 2015.

[53] N. Gupta, A. R. H. Fischer, and L. J. Frewer. Socio-psychological determinants of public acceptance of technologies: A review. *Public Understanding of Science*, 21(7):782–795, 2012.

[54] R. Halperin and J. Backhouse. A Qualitative Comparative Analysis of Citizens' Perception of eIDs and Interoperability. Technical Report 507512, FIDIS, 2009.

[55] M. Harbach, S. Fahl, M. Rieger, and M. Smith. On the acceptance of privacy-preserving authentication technology: The curious case of national identity cards. In M. D. Cristofaro and M. Wright, editors, *Proceedings of PETS'2013 – the 13th International Symposium on Privacy Enhancing Technologies Symposium*, volume 7981 of *Lecture Notes in Computer Science*, pages 245–264, Berlin, Heidelberg, New York, 2013. Springer.

[56] P. Harwood. Diffusion of the estonian id-card and its electronic usage: Explaining the success story. Master's thesis, Tallinn University of Technology, 5 2016.

[57] M. Järvsoo, A. Norta, V. Tsap, I. Pappel, and D. Draheim. Implementation of information security in the EU information systems: an Estonian case study. In S. A. Al-Sharhan, A. C. Simintiras, Y. K. Dwivedi, M. Janssen, M. Mäntymäki, L. Tahat, I. Moughrabi, T. M. Ali, and N. P. Rana, editors, *Proceedings of I3E'2018 – the 17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society: Challenges and Opportunities in the Digital Era*, volume 11195 of *Lecture Notes in Computer Science*, pages 150–163, Cham, 2018. Springer.

[58] O. Jokonya. Critical literature review of theory of planned behavior in the information systems research. In *Proceeding of AMEIT'2017 – the 2nd International Conference on Advances in Management Engineering and Information Technology*, pages 177–181. DEStech Transactions on Computer Science and Engineering, 2017.

[59] L. A. Jones, Antón, A. I., and J. B. Earp. Towards understanding user perceptions of authentication technologies. In P. Ning and T. Yu, editors, *Proceedings of WPES'07 – the 6xt ACM Workshop on Privacy in Electronic Society*, pages 91–98. Association for Computing Machinery, October 2007.

[60] T. Kalvet, M. Tiits, and K. Laas-Mikko. Public acceptance of advanced identity documents. In A. Kankanhalli, A. Ojo, and D. Soares, editors, *Proceedings of ICEGOV'18 – the 11th International Conference on Theory and Practice of Electronic Governance*, pages 429–432. Association for Computing Machinery, 2018.

[61] R. Kaplan. The role of empirical research in management accounting. Technical Report Working Paper 9-785-001, Division of Research, Harvard Business School, Boston, Massachusetts, 1985.

[62] H. Khan and A. Hutchison. Data privacy implications for security information and event management systems and other meta-systems. In M. Felici, editor, *Proceedings of CSP'13 – The 1st Trust in the Digital World and Cyber Security and Privacy EU Forum*, volume 182 of *Communications in Computer and Information Science*, pages 79–90, Berlin, Heidelberg, New York, 2013. Springer.

[63] B. A. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, Keele University, 2007.

[64] J. Koppenjan and J. Groenewegen. Institutional design for complex technological systems. *International Journal of Technology, Policy and Management*, 5(3):240–257, 2005.

[65] K. Kreos, E. Täks, V. Tsap, I. Pappel, and D. Draheim. On facilitating cross-border e-commerce through an automated VAT declaration system. In L. Terán, A. Meier, and J. Pincay, editors, *Proceedings of ICEDEG'2019 – the 6xt International Conference on eDemocracy & eGovernment*, pages 56–63. IEEE, 2019.

[66] A. Kütt and J. Priisalu. Framework of e-government technical infrastructure. case of estonia. In *Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE)*, page 1, 2014.

[67] P. Lan. A review of advantages and disadvantages of three paradigms: positivism , interpretivism and critical inquiry. Technical report, The University of Adelaide, April 2018.

[68] B. Latour. *Reassembling the Social: an Introduction to Actor-Network Theory*. Oxford University Press, 2005.

[69] M. Lips. Rethinking citizen-government relationships in the age of digital identity: Insights from research. *Information Polity*, 15(4):273–289, 2010.

[70] S. Lips, K. Aas, I. Pappel, and D. Draheim. Designing an effective long-term identity management strategy for a mature e-state. In A. Kõ, E. Francesconi, G. Anderst-Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2019 – the 8th Conference on Electronic Government and the Information Systems Perspective*, volume 11709 of *Lecture Notes in Computer Science*, pages 221–234, Berlin, Heidelberg, New York, 2019. Springer.

[71] S. Lips, V. Tsap, I. Pappel, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In A. Kõ and E. Francesconi, editors, *Proceedings of EGOVIS'2018 - the 7th International Conference on Electronic Government and the Information Systems Perspective*, volume 11032 of *Lecture Notes in Computer Science*, pages 60–70, Cham, 2018. Springer.

[72] V. M. Lockton. *e-Government and Identity Management in British Columbia: Implementation of the BCeID*. University of British Columbia, 2009. Master Thesis.

[73] N. Mackenzie and S. Knipe. Research dilemmas: Paradigms, methods and methodology. *Issues In Educational Research*, 16(2):193–205, 2006.

[74] A. R. Mærøe, A. Norta, V. Tsap, and I. Pappel. Increasing citizen participation in e-participatory budgeting processes. *Journal of Information Technology & Politics*, 18(2):125–147, 2021.

[75] I. Mariën and L. Van Audenhove. The Belgian e-ID and its complex path to implementation and innovational change. *Identity in the Information Society*, 3(1):27–41, 2010.

[76] T. Martens. Electronic identity management in estonia between market and state governance. *Identity in the Information Society*, 3(1):213–233, 2010.

[77] K. McBride, A. Kütt, S. Ben Yahia, and D. Draheim. On positive feedback loops in digital government architecture. In *Proceedings of the 11th International Conference on Management of Digital EcoSystems*, pages 174–180, 2019.

[78] K. McBride, Y. Misnikov, and D. Draheim. Discussing the foundations for interpretivist digital government research. In Y. Charalabidis, G. Pereira, and L. Flak, editors, *Scientific Foundations of Digital Governance*. Springer, Berlin, Heidelberg, New York, 2022. [forthcoming].

[79] K. McGrath. Identity verification and societal challenges: Explaining the gap between service provision and development outcomes. *MIS Quarterly*, 40(2):485–500, 2016.

[80] E. McLellan, K. M. MaCqueen, and J. L. Neidig. Beyond the qualitative interview: Data preparation and transcription. *Field Methods*, 15(1):63–84, 2003.

[81] U. Melin, K. Axelsson, and F. Söderström. Managing the development of e-ID in a public e-service context. *Transforming Government: People, Process and Policy*, 10(1):72–98, 2016.

[82] E. Mergenthaler and C. H. Stinson. Psychotherapy transcription standards. *Psychotherapy Research*, 2(2):125–142, 1992.

[83] Ministry of Economic Affairs and Communication. Estonian populations' satisfaction with public e-services 2014. Technical report, Ministry of Economic Affairs and Communications, 2014.

[84] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine*, 151:264–269, 2009.

[85] A. Muldme, I. Pappel, M. Lauk, and D. Draheim. A survey on customer satisfaction in national electronic ID user support. In *Proceedings of ICEDEG'2018 – the 5th International Conference on eDemocracy & eGovernment*, pages 31–37. IEEE, 2018.

[86] W. Nasri. Citizens' e-government services adoption: An extension of unified theory of acceptance and use of technology model. *International Journal of Public Administration in the Digital Age (IJPADA)*, 1(2):80–96, 2014.

[87] G. Ng-Kruelle, P. A. Swatman, J. F. Hampe, and D. S. Rebne. Biometrics and e-identity (e-passport) in the European Union: End-user perspectives on the adoption of a controversial innovation. *Journal of Theorectical and Applied Electronic Commerce Research*, 1(2):12–35, 2006.

[88] Nortal. Smart-id: Advanced electronic identity goes mobile. [last accessed 25/11/2021].

[89] L. Northrop, P. Feiler, R. P. Gabriel, J. Goodenough, R. Linger, T. Longstaff, R. Kazman, M. Klein, D. Schmidt, K. Sullivan, and K. Wallnau. Ultra-Large-Scale Systems - The Software Challenge of the Future. Technical report, Software Engineering Institute, Carnegie Mellon, June 2006.

[90] D. of State Information Systems. Information society yearbook 2009. Technical report, Ministry of Economic Affairs and Communications, 2009. https://www.digar.ee/arhiiv/et/download/214869.

[91] W. J. Orlikowski and J. J. Baroudi. Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, 2(1):1–28, 1991.

[92] M.-L. Palgin. *Diffusion of the Estonian ID-Card and Its Electronic Usage: Explaining the Success*. Tallinn University of Technology, 2016. Master thesis.

[93] I. Pappel, V. Tsap, and D. Draheim. The e-LocGov model for introducing e-governance into local governments: an Estonian case study. *IEEE Transactions on Emerging Topics in Computing*, 9(2):597–611, 2021.

[94] I. Pappel, V. Tsap, I. Pappel, and D. Draheim. Exploring e-services development in local government authorities by means of electronic document management systems. In A. Chugunov, Y. Misnikov, E. Roshchin, and D. Trutnev, editors, *Proceedings of EGOSE'2018 – the 5th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, volume 947 of *Communications in Computer and Information Science*, pages 223–234, Cham, 2019. Springer.

[95] A. Parsovs. *Estonian Electronic Identity Card and its Security Challenges*. PhD thesis, University of Tartu, 4 2021. University of Tartu Press.

[96] M. Patton. *Qualitative Research and Evaluation Methods – Integrating Theory and Practice, 4th edition*. SAGE Publications, November 2002.

[97] P. A. Pavlou and M. Fygenson. Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, 30(1):115–143, 2006.

[98] C. Perakslis and R. Wolk. Social acceptance of RFID as a biometric security method. *IEEE Technology and Society Magazine*, 25(3):34–42, 2006.

[99] Y. Petriv, R. Erlenheim, V. Tsap, I. Pappel, and D. Draheim. Designing effective chatbot solutions for the public sector: a case study from Ukraine. In A. Chugunov, I. Khodachek, Y. Misnikov, and D. Trutnev, editors, *Proceedings of EGOSE'2019 – the 6xt International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, volume 1135 of *Communications in Computer and Information Science*, pages 320–335, Cham, 2020. Springer.

[100] J. Platt. "Case study" in American methodological thought. *Current Sociology*, 40(1):17–48, 1992.

[101] O. Popelyshyn, V. Tsap, I. Pappel, and D. Draheim. On leveraging the potential of open data to enhance transparency and accountability – a case study from Ukraine. In L. Terán, A. Meier, and J. Pincay, editors, *Proceedings of ICEDEG'2019 – the 6xt International Conference on eDemocracy & eGovernment*, pages 25–30. IEEE, 2019.

[102] G. Robles, J. Gamalielsson, and B. Lundell. Setting up government 3.0 solutions based on open source software: The case of X-Road. In I. Lindgren, M. Janssen, H. Lee, A. Polini, M. P. R. Bolívar, H. J. Scholl, and E. Tambouris, editors, *Proceedings of EGOV'2019 – the 18th IFIP WG 8.5 International Conference on Electronic Government*, volume 11685 of *Lecture Notes in Computer Science*, pages 69–81, Berlin, Heidelberg, New York, 2019. Springer.

[103] E. M. Roggers. *Diffusion of Innovations, 4th ed.* Simon and Schuster, 2010. Free Press.

[104] H. Rossnagel, J. Camenisch, L. Fritsch, T. Gross, D. Houdeau, D. Huhnlein, A. Lehmann, and J. Shamah. FutureID - Shaping the Future of Electronic Identity. *Datenschutz und Datensicherheit*, 36, 2012.

[105] M. Ruus, I. Pappel, V. Tsap, and D. Draheim. Enhancing public e-service delivery: Recognizing and meeting user needs of youngsters in Estonia. In D. A. Alexandrov, A. V. Boukhanovsky, A. V. Chugunov, Y. Kabanov, O. Koltsova, and I. Musabirov, editors, *Proceedings of DTGS'2019 – the 4th International Conference on Digital Transformation & Global Society*, volume 1038 of *Communications in Computer and Information Science*, pages 29–40. Cham, 2019.

[106] A. A. Sai. An exploratory study of innovation adoption in Estonia. *Open Journal of Business and Management*, 6(4):857–889, 2018.

[107] E. Sau. The Estonian eID: a joint effort. Keesing Platform. [last accessed 25/02/2019] https://platform.keesingtechnologies.com/the-estonian-eid-a-joint-effort/.

[108] P. Seltsikas and R. M. O'Keefe. Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems*, 19(1):93–103, 2010.

[109] A. Seven et al. *Building sustainability and trust in the usage of electronic identification using technology acceptance model*. PhD thesis, Universitat Jaume I, 2015.

[110] L. Sjöberg. Attitudes toward technology and risk: Going beyond what is. *Policy Sciences*, 35:379–400, 2002.

[111] H. Snyder. Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104:333–339, November 2019.

[112] E. Stone. *Research Methods in Organizational Behavior*. Scott, Foresman and Company, Glenview, Illinois, 1978.

[113] T. D. Susanto and M. Aljoza. Individual acceptance of e-government services in a developing country: Dimensions of perceived usefulness and perceived ease of use and the importance of trust and social influence. *Procedia Computer Science*, 72:622–629, 2015.

[114] H. Taherdoost. A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, 22:960–967, 2018.

[115] M. Tiits, T. Kalvet, and K. Laas-Mikko. Social acceptance of ePassports. In A. Brömme and C. Busch, editors, *Proceedings of BIOSIG'2014 – the 9th International Conference of the Biometrics Special Interest Group*, volume P-212 of *Lecture Notes in Informatics*, pages 1–12. Gesellschaft für Informatik (GI), 2015.

[116] TNS Opinion & Social. Attitudes on data protection and electronic identity in the European Union. Technical Report Special Eurobarometer 359, European Commission – Directorate-General Communication, June 2011.

[117] V. Tsap. e-Identity and eIDAS: Interpretation of concepts by different countries. In A.-M. Osula and O. Maennel, editors, *Proceedings of ICR'2018 – the 4th Interdisciplinary Cyber Research Workshop 2018*, pages 9–10. Tallinn University of Technology, Department of Software Science, 2018. [last accessed 5 Nov 2021] https://haldus.taltech.ee/sites/default/files/2021-04/ICR2018_proceedings.pdf.

[118] V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2020 – the 9th International Conference on Electronic Government and the Information Systems Perspective*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer.

[119] V. Tsap, S. Lips, and D. Draheim. eID public acceptance in Estonia: towards understanding the citizen. In S.-J. Eom and J. Lee, editors, *Proceedings of dg.o'20 – the 21st Annual International Conference on Digital Government Research: Intelligent Government in the Intelligent Information Society*, pages 340–341. Association for Computing Machinery, 2020.

[120] V. Tsap and I. Pappel. Roundtable: Maturity of national eIDs. In *Abstracts of Papers Presented at the 18th European Conference on Digital Government ECDG 2018: University of Santiago de Compostela Spain, 25-26 October 2018*, page 46. Academic Conferences and Publishing International Limited, 2018.

[121] V. Tsap, I. Pappel, and D. Draheim. Key success factors in introducing national e-identification systems. In T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, editors, *Proceedings of FDSE'2017 – 4th International Conference on the Future Data and Security Engineering*, volume 10646 of *Lecture Notes in Computer Science*, pages 455–471, Cham, 2017. Springer.

[122] V. Tsap, I. Pappel, and D. Draheim. Factors affecting e-ID public acceptance: A literature review. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2019 – the 8th International Conference on Electronic Government and the Information Systems Perspective*, pages 176–188, Cham, 2019. Springer.

[123] M. Tsulukidze, K. Nyman-Metcalf, V. Tsap, I. Pappel, and D. Draheim. Aspects of personal data protection from state and citizen perspectives – case of Georgia. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, and M. Mäntymäki, editors, *Proceedings of I3E'2019 – the 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society: Digital Transformation for a Sustainable Society in the 21st Century*, volume 11701 of *Lecture Notes in Computer Science*, pages 476–488, Cham, 2019. Springer.

[124] A. Valtna-Dvořák, S. Lips, V. Tsap, R. Ottis, J. Priisalu, and D. Draheim. Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2021 – the 10th International Conference Electronic Government and the Information Systems Perspective*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer.

[125] D. van Rooy and J. Bus. Trust and privacy in the future Internet – a research perspective. *Identity in the Information Society*, 3(2):397–404, 2010.

[126] V. Venkatesh. Technology Acceptance Model and the unified theory of acceptance and use of technology. 7, January 2015.

[127] V. Venkatesh and H. Bala. Technology Acceptance Model 3 and a research agenda on interventions. *Decision Sciences*, 39(2):273–315, 2008.

[128] V. Venkatesh and F. D. Davis. A Model of the Antecedents of Perceived Ease of Use: Development and Test*. *Decision Sciences*, pages 451–481, 1996.

[129] V. Venkatesh and F. D. Davis. A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2):186–204, 2000.

[130] V. Venkatesh, M. Morris, G. Davis, and F. Davis. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3):425–478, 2003.

[131] V. Venkatesh, J. Y. L. Thong, and X. Xu. Consumer acceptance and use of information technology. *MIS Quarterly*, 36(1):157–178, 2012.

[132] S. Vlassenroot, K. Brookhuis, V. Marchau, and F. Witlox. Towards defining a unified concept for the acceptability of intelligent transport systems (its): A conceptual analysis based on the case of intelligent speed adaptation (isa). *Transportation Research Part F: Traffic Psychology and Behaviour*, 13(3):164–178, May 2010.

[133] J. vom Brocke, A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven. Standing on the shoulders of giants: Challenges and recommendations of literature search in information systems research. *Communications of the Association for Information Systems*, 37:205–224, August 2015.

[134] M. Warkentin, D. Gefen, P. A. Pavlou, and G. M. Rose. Encouraging citizen adoption of e-government by building trust. *Electronic Markets*, 12(3):157–162, 2002.

[135] A. T. Wessells. Reassembling the social: An introduction to actor-network-theory by bruno latour. *International Public Management Journal*, 10(3):351–356, 2007.

[136] O. E. Williamson. Transaction-cost economics: The governance of contractual relations. *The Journal of Law and Economics*, 22(2):233–261, 1979.

[137] O. E. Williamson. Transaction cost economics: How it works; where it is headed. *De Economist*, 146(1):25–58, 1998.

[138] R. Yin. *Case Study Research – Design and Methods*. SAGE Publications, 1984.

[139] R. K. Yin. *Case Study Research and – Design and Methods*, *6th ed*. SAGE Publications, 2019.

Acknowledgements

I would like to express my gratitude to my supervisor Dirk Draheim who has been endlessly supportive and patient through my entire PhD journey. His academic excellence, knowledge, and ethics guided and motivated me. I thank for the many hours spent on sharing invaluable insights and explaining complex things in a simple way.

I am also grateful to my co-supervisor Ingrid Pappel who encouraged me to begin this journey and later provided me with so many opportunities that equipped me with invaluable experience.

I thank my colleagues from Taltech who were so supportive, helpful, and fun to work with side-by-side.

My biggest gratitude goes to my parents, especially to my late mother who unconditionally believed in me from the very beginning even when I myself felt so down. I am positive she would have been very proud of me. I feel incredibly lucky to share this personal victory with my father whose love and support I always sense despite the kilometres between us.

A special and warm "thank you" is meant for my dear partner, friend, and soulmate who has been there through my highs and lows. It is one of the best feelings knowing someone is sure you will make it through and is ready to share your happy- and not-so-much moments.

Lastly, I thank my friends who were by my side. In fact, I thank anyone who has ever said any kind word of support that one way or another added up to my grit and perseverance, patience, and self-confidence.

This has been an extremely valuable and challenging thing for me to accomplish.

Thank you!

Valentyna Tsap
2022

Abstract
eID Public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity

The Estonian eID has been one of the most advanced national electronic identity systems by far. It is recognized as a part of the national critical infrastructure. The government of Estonia runs smoothly online, thousands of public and private e-services are delivering value to citizens who extensively use their eIDs making various transactions. Using the existing body of knowledge about electronic identity, we approach it from the perspective of the user and conduct the first comprehensive study on eID public acceptance. The aim of this dissertation is to unfold and examine how and why public acceptance of eID impacts the success of e-government. We employ a case study methodology to obtain a deep understanding of the subject. We identify what the eID public acceptance factors are by means of systematic literature review, and utilise the derived factors to target, interpret, and understand the Estonian citizens' perceptions of, and attitudes towards eID. We then validate our findings through thematic analysis of in-depth interviews with the top experts in the field, who explain and report on the importance of eID public acceptance in the overall success of e-government. We use institutional design analysis to position eID public acceptance as a crucial part of a large-scale information e-government system.

Kokkuvõte

eID avalik aktsepteerimine: edutegurid, kodanike pertseptsioon ja elektroonilise identiteedi mõju

Eesti eID on olnud üks kõige arenenumaid riiklike elektroonilise identiteedi süsteeme. Seda loetakse riiklikult kriitilise infrastruktuuri osaks. Eesti valitsus toimib sujuvalt internetipõhiselt, tuhanded avaliku ja erasektori e-teenused pakuvad väärtust kodanikele, kes kasutavad ulatuslikult oma elektroonilist identiteeti erinevate transaktsioonide tegemiseks. Kasutades olemasolevat teadmiste kogumit elektroonilise identiteedi kohta, läheneme sellele kasutaja perspektiivist ja viime läbi esimese põhjaliku uuringu eID avaliku aktsepteerimise kohta. Lõputöö eesmärk on uurida kuidas ja miks eID avalik aktsepteerimine mõjutab e-riigi edukust. Rakendame juhtumiuuringu meetodit, et sellest teemast sügavuti aru saada. Kirjanduse ülevaate abil tuvastame, mis on eID avaliku aktsepteerimist mõjutavad tegurid ja kasutame tuletatud tegureid, et tuvastada, tõlgendada ja mõista Eesti kodanike pertseptsiooni ja hoiakut eID-sse. Seejärel valideerime leiud oma ala tippekspertidega tehtud põhjalike intervjuude temaatilise analüüsi abil. Intervjuude käigus selgitavad eksperdid eID avaliku aktsepteerimise tähtsust üleüldise e-riigi edukuse kontekstis. Kasutame institutsionaalse disaini analüüsi, et näidata kui oluline osa on eID avalik aktsepteerimine laialdasest e-riigi infosüsteemist.

Appendix 1

I

V. Tsap, I. Pappel, and D. Draheim. Key success factors in introducing national e-identification systems. In T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, editors, *Proceedings of FDSE'2017 – 4th International Conference on the Future Data and Security Engineering*, volume 10646 of *Lecture Notes in Computer Science*, pages 455–471, Cham, 2017. Springer

Key Success Factors in Introducing National e-Identification Systems

Valentyna Tsap(✉), Ingrid Pappel, and Dirk Draheim

Tallinn University of Technology, Tallinn 12616, Estonia
valentyna.tsap@ttu.ee

Abstract. The following article seeks to investigate what the main success factors are when implementing national e-identification systems as a part of e-governance strategies. The article reviews the case of Ukraine that currently is in the beginning of e-identification management system deployment. In frames of the paper, positive experience of foreign countries in electronic identity management is examined aiming to outline lessons that can be learned by Ukraine. The article aims to identify main issues and problems that inhibit the development of successful e-identification system in Ukraine assuming citizens' awareness as one of the key success factors. Positioning it as a crucial factor is underpinned by means of conducting a survey among Ukrainian citizens. Based on conducted interviews with officials, a local government e-identity solution is discussed as a project that can be potentially applicable on a national level. Personal vision of authors on improving and raising citizens' awareness on e-government and e-identification is presented as a recommendation for stakeholders' consideration, being at the same time a hypothesis for future studies.

Keywords: E-Government · ID card · Citizens' awareness

1 Introduction

Today, technologies determine a large part of success of most of the countries. Moving to digitalization is one of the important issues nowadays, and governments take this concern very seriously since e-governance proved itself to be a recognized tool of running the state in a smart and efficient way. One of the most important components of e-government is e-identification as it facilitates access to e-services that are delivered to citizens. Besides, it also allows paperless management as a foundation for digitalized government which has successfully been implemented, for instance, in Estonia relatively not a long time ago [5, 10] Countries whose citizens own ID cards accessing public e-services, showed that e-identity has to be one of the top priorities when it comes to building an e-state.

This paper aims to provide an overview of key elements of e-identification systems based on the lessons learned from countries that have already established them in the context of e-governance development, distinguishing citizens' awareness as a substantial component of successful implementation. The matter of awareness will be presented and discussed in frames of the case of Ukraine underpinned by the survey

T.K. Dang et al. (Eds.): FDSE 2017, LNCS 10646, pp. 455–471, 2017.
https://doi.org/10.1007/978-3-319-70004-5_33

results of which contribute to the evaluation of citizens' awareness level towards e-identification and e-governance in general.

Ukraine, an Eastern European country, one of the developing states that has proclaimed e-government establishing as one of the prioritized areas relatively not a long time ago. Ukrainian government is already working on implementing eIDs, however, this is considered to be a very early stage of the process, and the citizens are not familiar with possibilities and benefits which they can receive when they will switch to plastic cards, as it was discovered during the survey conduction. Knowing how to deliver e-identity as a concept and as a product to population has to be one of the biggest concerns of the government if they are willing to success in this project. Currently, in Ukraine, this issue is somewhat being neglected, and this fact accumulates a threat of reluctance using ID card and, as consequence, e-services. Moreover, the analysis of the research results have identified significant trust issues from citizens' side towards government. This is rather not a discovery but a common knowledge due to the actuality of this problem that underlies in relations between people and authorities caused by various factors that go back deep to the history and culture of Ukraine. The problem of awareness and trust are explicitly coherent and bring up additional obstacles when it comes to dealing with technological component in public sector.

As the country is already having emerging e-government projects of different scale, their stakeholders were interviewed in order to receive an opinion on the most influential factors when running such projects, including the issue of citizens' awareness.

Based on the findings of the research and international experience, within this article we will present a set of recommendations on how to raise citizens' awareness towards e-identification and e-governance, in general.

In Sect. 2 we will provide an insight of current developments in e-identification in Ukraine along with the comparison to other countries' experiences in this field. In Sect. 3 we will discuss the results of conducted survey and interviews on citizens' awareness towards eID and e-governance in Ukraine and local e-identity solution in one of the cities of Ukraine. Based on the findings, Sect. 4 will represent main obstacles and difficulties that concern the researched area and awareness issue specifically. Based on the analysis of abovementioned, recommendations for improvements and outline of future research will be drawn in Sect. 5. The paper will be finished with a description of related works in Sect. 6 and a conclusion in Sect. 7.

2 e-Identification in Ukraine

The matter of e-identification in Ukraine is urgent in terms of political and economic integration with EU, and also taking into account the growing penetration of technologies into people's lives, society and economy digitization. The lack of a common approach in this matter have led to a situation where in systems that are used for different purposes and scale use means of electronic identification without complying the basic requirements in security, protection of personal data, trusted identification and authentication, interoperability, accessibility and usability. Solving problems associated with implementation of e-identification technologies by means of regional or sectoral management is rather inefficient as it contradicts with the idea of aggregated and comprehensive e-services provision in frames of appropriate legislation and technical regulations, coordination of measures, which are aimed to solve the problems according to the concept of information society, cybersecurity, socioeconomic problems focusing on integration to a single European market. The main and the most urgent factor that spurs these processes in Ukraine is recently adopted 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 was adopted that has repealed Directive 1999/93/EC [7]. The provisions of eIDAS regulation cover two main areas: electronic identity and electronic services. The overall goal is to reach cross-border interoperability.

Formulation of Ukrainian national legislation in the field of e-identity, e-signature and e-services has to take place taking into account eIDAS regulation and be based on it. It is crucial to ensure legal interoperability of e-identity and trust services schemes already during the development phase [13].

Going further to ID cards in Ukraine, the project itself was launched in fall 2016. According to the State Migration Service of Ukraine, the plastic passport is issued as a plastic card with embedded electronic chip. The new ID contains the name of the country, name of the document, name, sex, citizenship, date of birth, unique registry number, number of the document, expiration date, date of issue, name of entity that issued, place of birth, signature and photo. The information that will be stored on the electronic chip will include marital status and place of residence information, e-signature (optional), biometric data (optional). To update or insert new personal information will be possible by submitting a solicitation; however, it's not applicable to the registry of place of residence [17].

It is planned that paper passports will be replaced by plastic ones during 5 years and, hence, there is no need for citizens to do it immediately. An important aspect that has to be outlined is the fact that if a person due to her religious beliefs will have a right to refuse to receive a document with electronic identifier by submitting a relevant application. The document will be issued and valid for 10 years [19].

2.1 E-ID Management Experience in Different Countries

In the context of the topic below an overview and comparison of different countries' experiences in the field of eID management will be presented. The countries chosen for this analysis are as follows: Estonia, Austria, Sweden and India representing Northern and Central Europe and Asia. Each of these countries has their own history and path that it has taken to implement the electronic identification in frames of e-state.

The below Table 1 will serve as a short descriptive introduction that will allow to receive a general understanding of differences between specifications of eID cards that each of these countries issues to their citizens.

So far, among European countries Estonia has been the most successful one in spreading eID to population, mostly because it is simply mandatory, and, in the beginning of the project, inclusion of banking sector to the process was the most remarkable step that ensured ubiquity of eID in a relatively short time period [12]. Also, Estonia focused first on the building the interoperability between different systems based

Table 1. Overview of eID

Criteria/Country	Estonia	Austria	Sweden	India
Number of tokens	1	>1	>1	1
Mandatory	Yes	No	No	Yes
Contact chip	Yes	Yes	Yes	No
e-Signature	Yes	No	No	Yes
Biometrics	No	No	No	No
Payment transaction	No	Yes	Yes	Yes

on X-road which has been serving as basis for Estonian e-Governance [5]. In this sense, India has also shown a great ability to fulfil ambitious goals of its UID issuing them to over 1.3 billion of people in the country applying the "killer app" of micropayments and promoting the solution tackling relevant levers that spurred people to perceive it as an everyday utility [7, 8]. It can be stated that Austrian and Swedish eIDs are not so commonly used in comparison with other states taking into account the fact that in both countries do exist other types of tokens and authentication types, one of the most popular of which is BankID [9, 12–14]. Cases of India and Estonia are justified to be more successful when it comes to the spread of their eIDs because of the mandatory nature of those documents forcing population obtaining it and being encouraged by facilitating affordability, ease of use, advantages and transparent purpose. In other country cases, complexity of use, interoperability issues, existence of variety of alternative options may have also affect the level of eID use. Naturally, each country's historical, ethnical and cultural factors are also playing a significant role in this context [6].

Yet, if we compare those country profiles to Ukraine, the latter's level of development is naturally quite low, obviously, not only due to the novelty of the project but also to lack of infrastructure, legislation superficiality and shallowness and many other reasons. Considering foreign experience in this field for Ukraine is crucial.

3 Citizens' Awareness as One of the Potential Key Success Factors in e-Identification in Ukraine

In this chapter will be provided the outcomes of the survey for citizens of Ukraine aiming to identify their current level of awareness towards e-governance and e-identification; moreover, a concrete case regarding the Lviv citizen card which has been implemented in Lviv as a tool for identity management for public service provision purposes will be introduced. The questionnaire has been distributed via internet using social networks and email channels; the interviews have also been conducted online.

3.1 Citizens' Attitudes Towards EID in Ukraine

The questionnaire consisted of 14 positions that, in general, had a purpose to receive basic information about citizens' opinions, attitudes, concerns, interests, access to various resources in terms of the given field, their feedback etc.

Delving into details and results, to start with, the age of responders was requested to be specified, hence, the results show the majority of responders were aged 21–40 y. o. which is 66, 2% from the total number of people who submitted their reply. Going further, the next age group was 41–50 (15% of responders) and 50 y. o. and higher (12, 2%) which is a larger number of respondents aged 14–20 y. o. (6, 3%).

Moving forward, the next issue that was found out during result analysis is that people when turning to governmental institutions experiencing lines very often and only few have confirmed that they either do not face it often or not at all; some have used an option of electronic line if it was available.

Such numbers definitely prove that government institutions cannot process the current flow of citizens' requests which can be explained by already discussed reasons such as bureaucracy, unnecessary complexity, lack of communication within governmental departments etc. These causes could be potentially eliminated by means of e-state attributes and ICT, in general.

Considering the current existence of some electronic public services and their use, citizens were asked about it, and the correlation between positive and negative responses is somewhat overwhelming: 79, 3% do not know such services exist. This indicator can be used when assuming with a high level of confidence that, even though the development of e-government has started, such component as informing citizens about new possibilities is being let out of attention.

People were asked which e-services they have already used amongst those that exist so far, and result have shown that 23, 9% were using the opportunity to fill in required documents in advance to bring them later to governmental offices. 24, 8% of respondents were authenticated to portals and sent their requests online. A minority of 5% of respondents failed to request a service online due to its unavailability in their region. The rest, which is nearly half of respondents, didn't use any e-services. It has to

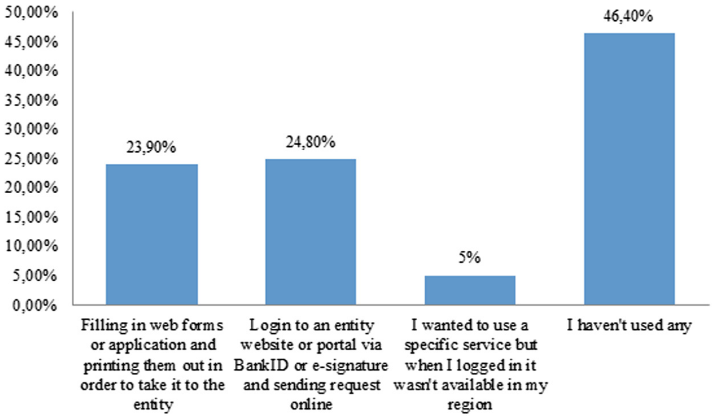


Fig. 1. What public e-services you have used already?

be pointed out that those websites that provide the possibility to make an administrative request still lack the attribute of ubiquity and accessibility, so those who refer, for example, igov.org.ua, the most commonly known e-services portal, more than often find out that this particular service they want to use is not available in their area. This leads, naturally, to dissatisfaction and fails people's expectations towards state's performance and losing trust to it (Fig. 1).

Consequently, the next question's results about people's trust to e-services show that the trust itself cannot be something the can people feel towards what they don't know about or if it can't be experienced. This is why 29% answered that they actually trust e-services, 64% trust only partially and the rest doesn't trust them at all (Fig. 2).

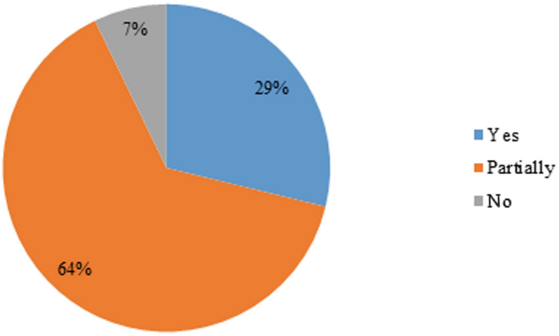


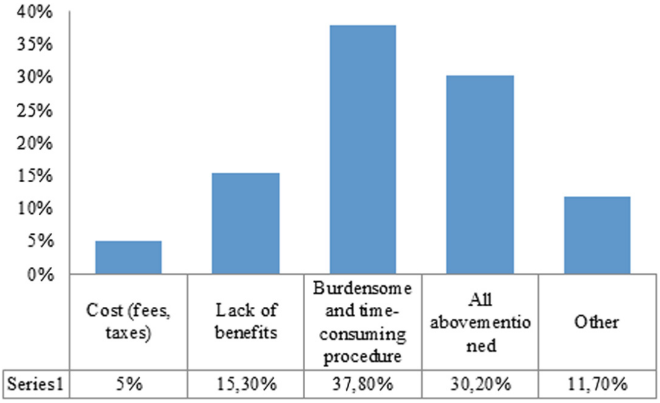
Fig. 2. Do you trust e-services?

The next section of survey was dedicated to ID passports and aspects of national identification. Even though the ID-passport has started to be issued less than a year ago, when respondents were asked what national ID document they are holding now, 8 of 222 answered they already have a new format plastic passport. 81% confirmed they have a regular paper passport, and the rest 15, 3% informed they use driving license as an identification document.

People were asked both reasons why they would change their passport to a new ID card and why would they prefer not to do that. The first question has brought the following results.

Almost half of respondents beliefs that new ID card is expected to be used to reach government services online, but there is a significant part of them (31%) who have to intention to get a new ID card, while the other 2% do not know about such type of identification document. It is assumed that the change of existing passport is not a priority for Ukrainian citizen for many reasons. A large number of them will be dis-cussed below, but at this point it has to be mentioned that such reluctance can be explained by the government's positioning of the beginning of new ID issuance. To be more precise, they are informing that replacement of old format passport is not compulsory and the change will take place gradually, at least 5 years. Despite the fact that paper passports will not be issued anymore to young people who reached 14 years, yet, citizens who have to change their passport photo once they reaching age of 25 and 45 years will still have an opportunity just to replace the photo keeping the paper passport. Another important aspect that has already been pointed out above is that citizens are able to refuse to store their data electronically on the card by filling in a certain application. Such option is rather unreasonable in some sense since it inhibits various important processes which are, for example, the spread of e-solution that has numerous benefits as one of the core factors of e-government; pace of adaptation to a new standard document which is a factor of low awareness level cause. Moreover, in the future, if the state is able to provide services electronically, people who earlier were issued cards without a chip won't be able to access all benefits, and this can lead to unnecessary expenses both for citizens and government, performance of the identification system and citizens' satisfaction level.

Apart from that, answers of respondents show that what most stops them to change their passport is time-consuming procedure that is associated with collecting various paper documents. The other part of respondents considers there are no benefits in doing so. Only 5% replied that they would not start the procedure due to the state fee. Third part of the total number of respondents replied choosing all options mentioned, and 11, 5% have named other reasons that preventing them to replace current IDs, for example, someone didn't know about such opportunity or explained that since there is a very low level of development of required infrastructure, the new ID won't have any advantages (Fig. 3). Three respondents, who have left a comment, informed that they do not trust the country and government.



	Cost (fees, taxes)	Lack of benefits	Burdensome and time-consuming procedure	All abovementioned	Other
Series1	5%	15,30%	37,80%	30,20%	11,70%

Fig. 3. What is preventing you to change your passport to an ID card?

The next set of questions is concerning technical specifications of ID card; The aim was to have a better understanding of people's attitude towards some potentially sensitive matters that are usually present when a new technological solution is being implemented. Moreover, realizing the background factors that cause these attitudes as this can serve as an area for improvements striving to lean them towards a positive side.

People were asked whether they are aware of what an electronic signature is, and it can be presumed, that due to its implementation which started back into 2003, respondents' replies show that 63, 1% know what it is though don't use it; 22, 5% do not know about it; 14, 4% are actually using it. Taking into account a relatively high level of awareness on e-signature, it can be argued that this simplifies and speed the process of acceptance and adaptation of new-format document. Being a core element of electronic identification, there has to be a big emphasis on e-signature, raising awareness of civil population, businesses and government side. Low percentage of those who uses electronic signature nowadays in Ukraine can be explained by a complex and long procedure of receiving a certificate, interoperability issues, ease of use matters, etc. Before starting taking measures to encourage not only entities use it but citizens as well, the entire field has to go from top to bottom through a set of reforms simplifying the complex procedures and regulations, mainly legislative and technical ones.

While learning electronic identification document attributes and international experience in using different standards within the given topic it was decided to include also a position about storage of biometrics. Major number of respondents (62, 2%) answering the question would they agree their biometric data to be stored on national ID cards, thought positive, considering such attribute as an additional level of protection and higher standard of identification. Almost all the rest of the respondents (32, 9%) would not want their data to be stored in government databases. 2, 7% replied they do not know or didn't understand what it is. 5 respondents answered this is against their religious beliefs. Such results, ambiguously, confirm that people care about security of their personal information but if the major part has an understanding how it works when it comes to this solution, yet, questioning state's ability to guarantee security. This allows suggesting putting additional efforts and attention to a matter of data protection provisions and their delivery to citizens ensuring their awareness on it.

Continuing with the technical specifications of eID, respondents' answers for the question on would they prefer eID as means of authentication when accessing e-services, have drawn the following picture.

Nearly half of the people answered they would prefer to use ID card to confirm their identity; 14% mentioned that this option wouldn't be suitable for them as in some situations there is need to ask for an advice or help from official. Yet, 21% would choose to authenticate themselves by means of username and password. Here, it has to be mentioned, that, presumably, people chose this method because of its ease of use, however, there are high risks of identity theft associated with it. Thus, occurrence of cybersecurity breaches and fraud risks have to be explained to population whilst stressing on the means with higher level of safety use. Going further, 6% would use alternative methods, which currently, most common one is BankID. 10% of respondents confirmed it is easier for them to go personally to the government office.

Generalizing, 90, 1%, which is 200 of respondents, confirmed that they would use governmental e-services rather than going to administrative centres and offices. The rest 9, 9% would prefer things to remain as they are right now. Naturally, citizens' opinion shows that the problem which is being researched within the paper is urgent and positive changes required and expected.

Additionally, within the conducted survey, respondents were given an opportunity to share their thoughts, feedbacks or comments which were submitted by 15 of them. Having analysed the submitted comments, several of them relate to particular issues such as low level of e-services development and e-government in general; inefficiency of authority; the matter of trust to government. Moreover, feedbacks on using existing electronic authentication methods and e-services portals were left, confirming their satisfaction with the ability to do it remotely and much faster.

It can be confidently argued that even though the scale of conducted survey might not bring fully objective results, but it is clear that the situation with people's realization of upcoming changes is urgent and requires actions. Going further with the research, a local e-government project implemented by the City Council of Lviv will be presented as an e-identification solution that provides benefits to citizens of Lviv.

3.2 Lviv Citizen Card: Local E-Government Solution and Stakeholders' Opinion on Future Challenges

Currently, in Ukraine e-government solutions on local level are being implemented fragmentally and scattered. When it comes to e-identity, there a few cities that have already started to work on projects that aim to bring existing electronic services to citizens without a need to visit administrative service centers. The cities which already have more or less mature concept are Kyiv, Lviv and Dnipro. This subsection will give an overview about Lviv case based on the conducted interviews with general managers and developers of the project. The members of the project were asked a set of specific questions regarding it aiming to build a basic understanding of the current developments in e-governance on the local level.

Located in the Western Ukraine, Lviv is considered to be one of the cities with a high level of public activity where citizens proactively participate in public life.

The idea of the project was established in 2015 as a potential solution for all Lviv citizens but back in that time, it aimed to be issued to members of antiterrorist operation (ATO) that is still taking place in the conflict zone in the Eastern Ukraine [16]. The card itself is an identity document that can be used for accessing various services more effectively and efficiently. Initially, the card included services that are most relevant and demanded to the members of ATO, for instance, social protection and financial aid, but know, as the current manager of the project, Respondent 1, states, the card is will include more services that can be used by all citizens of the city. The card of citizen of Lviv is also a bank card which allows using it for financial operations. Hence, it contains an electronic chip that stores personal information and can contain certificates allowing it to be utilized for digital signatures as well. The data stored can be access by the official who extracts it by putting it into card reader device. As the general manager of the project informs, Lviv City Council is already equipped with required infrastructure in order to ensure the delivery of services and operating with information online.

As it was just mentioned above, the card allows requesting social protection services and financial aid which normally is followed by collection of a number of applications but once the card was issued, the owner will be able to do it skipping this step as all information will be stored in the system. Moreover, being a bank card of one of the biggest banks in Ukraine it allows the owner to identify himself with BankID and access e-services in their personal account on the city council's website. Furthermore, the owner of the Lviv citizen's card is able to use public electric transportation free of charge.

The current manager of the project has informed that the project is being on its pilot stage. So far, the card could be used by ATO members but now the team is working on scaling it for every average citizen along with enabling to use a larger range of e-services. To be more precise, currently, an e-ticket for public transportation with the possibility of contactless payment is being implemented. The former manager of the project, Respondent 2, states that this is one of the advantages of this card - it can be used as e-ticket and also can be used for electronic signatures as it contains certificates by one of the banks. At the moment, more than two thousand cards have been issued.

During the interview, the interviewees were asked what were and are currently the biggest obstacles and difficulties for them as service providers. All three respondents named various reasons but the common one was the lack of a single identifier and a unified database and electronic document exchange system. The manager of the project states that, for instance, a person who holds Lviv Citizen Card requests a service, the internal departments usually need additional information that is not stored within their access in their internal databases, so they are forced to make official requests to other state entities which significantly slows the delivery of service down along with its efficiency. The former manager of the project also mentioned that there is no infrastructure developed and people do not own the card readers to use the full range of benefits. Moreover, if the Lviv City Council's services can be requested online, other public services are mostly not available at the moment. The Respondent 3, who deals with technical specifications, points out that another problem is the lack of understanding the aim of the project in certain departments or their reluctance to support its implementation. Answering the question about the potential possibility to scale this project on the national level, the respondents have ambiguous opinions. The current manager of the project mentioned that interoperability of their solution theoretically can be possible once other regions start design their own local solutions but it has a range of technical and bureaucratic issues that have to be solved. The Respondent 3, states that their solution is meant to be used on the local level while on the national newly implemented ID passport is ought to function as enabler of access to other public e-services.

Moving forward to people's awareness, the respondents were asked their opinion on this matter and its importance for the success of e-government solutions. All of them have agreed that this aspect plays on of the key roles when running the discussed solutions as it has to be kept in mind that not only this is implemented for the state effectiveness increase but for citizens since they are the "end users and customers". Here we can refer to already mentioned concepts of good governance and new public management.

Going back to the Lviv Citizen Card, respondents were asked to provide information on the activities that were carried out by them aiming to inform the publicity raising their awareness towards this solution. Summarizing, it has been informed that the following activities were carried out such as media campaigns, press releases, reports on thematic conferences, social network announces, informing about new possibilities on sight, meaning all administrative service centers. The current manager of the project states that Lviv is a city where people are very active taking part in the public life of the city and are always interested in new implementations, especially, the younger generation; as Respondent 1 mentioned, youth values its time and, naturally, is more opened easier to accept innovations. When it comes, to elderly, the manager confirmed that the level of interest is not so high though it's there and is being encouraged.

In order to better understand how Lviv Citizen Card works, the responders described the process of providing an e-service takes place. The scheme below visual displays the mentioned process step-by-step, according to information received during the interview. The respondents have described a process of request of financial aid for a citizen. To start with brief explanation, the citizen has to show up to one of the administrative service centers and request this service in person because so far citizens do now own a special smartcard reader. Afterwards, citizen presents his card and by means of reader device the official accesses citizens' personal data stored in the card and checks if citizens' profile contains required documents that are needed to approve financial aid according to the procedures. If the necessary documents are already inserted to the system beforehand, the official processes the request and sends an approval to relevant department who is responsible for processing the transfers. In case some documents are missed, the official sends a request to departments who can provide such documents, and once they respond, the official, as it was already mentioned, processed the approval for transferring the amount to the citizen's bank account which in most cases is located in the bank who is cooperating with Lviv City Council and is responsible for issuing the cards.

In overall, all respondents agree that this project is still very "raw" and requires systematic reforms that are ought to be approved on the national level. Indeed, it can be argued that the above described project is very promising but without further actions on the national level it will not be possible to reach set goals.

Having analysed the primary data received during the conduction of survey and interviews, it can be summarized that gathered information is very valuable and allows building hypotheses and formulating recommendations on how to improve people's knowledge about e-governance and mainly e-identification, its advantages and opportunities. According to the hypothesis, the accent in recommendation should be put citizens' awareness as all in all, this aspect is not clearly outlined in any of the actions plans, strategies or policies.

4 Main Problems and Issues Arisen in This Research

As any other country, Ukraine is very special with its history, culture and population mentality that majorly define the core and essence of it. Having learned what is standing behind the domain that is being researched, as it was already said above, identity, within the state that is driven by the principles of good governance and the concept of new public management, by means of ICT, has been shifted to digital world becoming a component and a tool at the same time, of e-state. Going further, cases of countries from different regions of the world have also proven that having their own challenges, back in each of their times, India, Austria and Sweden have also managed to implement electronic identities tailoring the infrastructure to their needs. In each studied case it was discovered that in one way or another, countries have put their efforts not only to restructure and build legislation, develop technical side and infrastructure but also taking measures that ensure that their citizens will be encouraged and aware how to use new solutions understanding the agenda. Ukraine is characterized as a state that only has started to make first steps towards e-governance. Understanding the benefits and advantages, the government of Ukraine is striving to move forward and succeed but various issues and obstacles of different scale are preventing to do it currently. Seeking to find answers to research questions in frames of the article, Ukraine's specifications concerning e-identification were learned.

ID cards in Ukraine that were approved as a new format of National ID are aimed to be a tool for citizens that can be used by them accessing e-services. Being justified by a very early stage of development that is explained by a "raw" legislation and lack of infrastructure, yet it can already be stated that Ukraine has to put significantly more efforts in order to successfully implement and run electronic identification system. After analyzing the existent legislation on main components that are have to be included to e-identification and e-governance in general, adopted programs and action plans, it is argued that though and enormous amount of work is done already but because of its fragmental and superficial nature, a wide range of matter are being lost from sight which causes the current situation when objectively the overall level of success in this area is estimated to be very little.

Analysing the factors that influence the subject of this work, it was assumed that citizens' awareness on eID and e-governance in general is an important aspect that is somewhat neglected and has to be tackled by the government of Ukraine. By using the methodology described above, meaning the conduction of survey with citizens and interviews with officials involved in e-identity area, throughout the research several statements can be made based on the results and studying the materials on the current situation in Ukraine.

So far, Ukraine is risking failing at managing to establish the ID card project because a number of issues. This is a general statement that will be followed by arguments that underpin it specifying the mentioned issues.

Despite the fact that relevant regulations and action plans on matters related to e-governance and eID do exist already, authorities hesitate to implement and follow them. This mainly can be explained by a long history and tradition of running state errands that foster corruption, which, if it may be stated in such way, reached ridiculous level and, what is even worse, is sometimes taken as granted by people. It is known, that unfortunately, many politicians are driven by the personal advantage they want to receive which results in indifference to what is not concerning their interests and, hence, leads to problems in socioeconomic development and welfare.

4.1 Main Obstacles in Regards to the EID Awareness

Emanating from the previous statement, it has to be pointed out, also based on the results of survey, that Ukrainians, naturally, realize the abovementioned problem and the urge of changes. This can be also proven by the events that took place in Kyiv in the fall 2013 [18] that basically showed how much people did not trust government and politicians that ruled back at that time. As this turning point, since then, has caused some positive changes, yet people do not fully trust government. Going back to the subject of research, it has to be stated that because of strong trust issues chances for the implemented ID project to success are low so far.

This leads to another statement that underpins the focus: citizens are not fully informed about all aspects and reasons for implementing this solutions.

Due to the big percentage of respondents who informed that they are not aware of existing innovations and lack understanding of purpose or have concerns regarding data protection, citizens require more education in order to increase their digital literacy that directly impacts motivation to use new services online.

Results of interview show that on local level there are already initiatives driven by principles of transparency and efficiency but they are not able to develop and improve further because of the foundation which is legislation and infrastructure. This leads to fragmental and scattered developments of some solutions (volunteer projects, portals, initiatives etc.) that though might benefit the citizens but is rather creates a growing number of solutions that are not interoperable between each other and creates their unnecessary heterogeneity and variety, for instance, the number of already existing portable with public services or the number of certification centers.

The absence of citizen-centered approach that is supposed to put people's interests and needs in the front in terms of delivering public services, leads to already mentioned many times low awareness level.

Hence, it can be concluded the mentioned statements above are highly interconnected and emanate from each other. Referring again to results of questionnaire and interview, confidently, the citizens' awareness towards is one of the key aspects that have to be considered when implementing e-governance and its components.

In frames of the paper given above, the background idea of electronic identity and e-governance in general was discussed, followed by presenting international practice of electronic identity management, going further to the case of Ukraine, analyzing its existing implementations in e-identity area, outlined as a research question. Moving to the second research question, the issue of citizens' awareness towards eID and e-governance was put as a key aspect and factor of success when implementing such solution was aimed to identify during the research process. After conducting the re-search by means of qualitative methods, it was managed to prove citizens' awareness as one of the weak spots of Ukrainian electronic identity management and e-government strategy. Lastly, the third research question was to outline the lessons that had to be learned from positive experience of Estonia, Austria, India and Sweden whose practice differs but, has a significant level of acceptance among theirs citizens.

5 Recommendations

Delving into literature which was used to build the structure of this paper and formulating our arguments, we have encountered various contradictions, gaps and ambiguous aspects that have impacted the opinion and conclusions below.

After getting familiar with the case of Ukraine and identifying the specifications that determine the current state of its electronic identity management and the environment in which it exists and develops, an analysis of people's attitudes and awareness on the given subject was conducted. Moreover, a case of positive local government e-solution was described thanks to the officials who are directly involved in the project development and its maintenance.

Before presenting the measures and activities that have to be carried out by governments in order to raise people's awareness towards eID and e-governance in general and changing their attitudes, a set of prerequisites has to be presented. The reason of their implementation is that based on the international practices, it is clear that there are some general conditions of proper functioning of electronic identity management within a country. In case of Ukraine, the following prerequisites have to be met:

1. Harmonization of electronic identity management system with eIDAS Regulation;
2. Legislation that defines a unified identifier has to be adopted that will ensure successful and seamless operation with electronic entries that will be linked to a unique number; this will also benefit the unified electronic document exchange system which so far doesn't not exist;
3. Unified electronic document exchange system has to be implemented between the governmental authorities to facilitate secure and efficient data flow;
4. Amendment that will make ID passport a compulsory document format based on the experience of Estonia which was one of the conditions of ID card spread among the entire population;
5. Amendment to PKI legislation which will ensure a limited number of authorized certification authorities responsible for certificates issue; this has to be conducted for the sake of interoperability and guarantee of verification process;
6. Provision of the required equipment in all administrative centers to ensure the ability to operate with eID and delivery of services.

Currently, as it was mentioned before, Ukraine cannot fulfil these requirements instantly, and it will take year for these changes to take place. Furthermore, the already discussed above matter of common corruption phenomenon within state structures urges not only these prerequisites to be met, but rather a disruptive change to happen that would fundamentally redefine the way of running state errands eradicating the old routine. This statement is somewhat vague and indistinct based on personal vision but nevertheless has a right to take place in frames of the given research.

Herewith, aiming to change the citizens' attitudes and awareness towards eIDs and e-governance in general that would guarantee a higher level of their acceptance, the following recommendations are presented as follows:

A Concept on raising citizens' awareness on e-governance and increasing the level of digital literacy enhancing their computer skills and knowledge based on the approach of continuous learning models should be adopted. The Concept should include separate projects for different age categories of population personalizing methods of education to each of those.

The concept of public service provision on each level of government using citizen-centered approach and put in front people's interests and needs should be redefined. Lessons can be learned from private sector that is usually much more successful when meeting customer/user needs. This is also reasoned by the already mentioned concept of new public management.

Citizens must be ensured in the guaranteed security of their personal data retention transparently communicating main principles of cybersecurity making it one of the main basic prerequisites.

Running ubiquitous campaigns that positioning e-governance and, of course, eID as a prerequisite of transparent, effective, efficient and corruption-free government which will ensure the increase of citizens' trust towards it and will also give an insight of e-services and their benefits.

Development of a one-stop-shop web portal where all e-services will be gathered facilitating their access and ensuring a decent, clear and functional system of online assistance. Currently, those e-services that exist and can be used via online authentication are available only for few authorities' websites, often not fully functional and intuitively not clear how to use, lacking instructions.

The most important and perhaps the most challenging task for Ukrainian authorities is to ensure that all above mentioned will be provided in each region equally to every citizen, considering the size of the country and number of population.

It is understandable that the above measures require enormous resources and time but judging from practices of other countries, by systemized and precise policies and strategies that have clear goals it will guarantee positive changes.

6 Related Works

The matter of citizens' awareness towards e-governance is being discussed more often than before because of the ubiquitous application of innovations and ICT. Going through the international experience we can observe stakeholders raising this problem pursuing to identify the level of its impact and its importance for the success of the project. Most of the studies related to this topic are conducted within countries investigating each as a case study applying various analytical methods. For instance, the results of a study conducted in Jordan which evaluates awareness and acceptability of e-government services within the country [3], are similar to those that were received during the analysis of the case of Ukraine. To be more precise, both countries are in the beginning of the implementation phase and both samples shown that people are not informed about online opportunities that state is offering currently. Another study on citizens' perception towards e-governance conducted within United Arab Emirates by means of Likert scale that helped to come up with evaluation of several factors that influence citizens' attitudes, conducted by Al, concludes with almost identical statement that the core issue is the low level of citizens' awareness or either low level of trust towards government [2]. The materials that were used in frames of analysis of countries' experiences in this paper are giving an overview of e-identification implementation in each of the cases mentioning the component of eID project adaptation among population and presenting statistics on its relative acceptance. However, there are less academic sources regarding this matter that concern specifically e-identification rather than e-governance in general. Moreover, when it comes to Ukraine, due to the early stage of development of e-state, this topic is novel and requires further research in this domain to get a deeper insight. Hence, aside from findings which were identified during this research, the future ones will contribute to generalized knowledge in this field and will allow potential applications in other countries. All in all, similar research for other countries recognize the issue of awareness towards e-governance as one that demands attention of decision makers in order to reach higher level of acceptance, adaptation and success of information systems in public sector that are being implemented nowadays. Yet, when it comes to case studies of countries it is essential to keep in mind the influence ethnic and cultural factor as variables that fluctuate depending on each case which is also outlined in existing studies by researchers.

7 Conclusion

E-identification has already proven itself as an effective means or delivering and receiving public e-services in terms of e-governance. Nowadays, the majority of countries are striving to apply ICT in public sector focusing on multiple components such as legislation, technical standards, infrastructure and promotion. The latter sometimes doesn't have enough attention and resources dedicated to it. For instance, Estonia, one of the most successful countries in this sense, managed to achieve a high percentage of eID ubiquitous utilization by individuals and entities as an everyday utility. Other cases of countries that were mentioned in this paper have also shown that states spent resources to inform publicity about innovative way of interaction with public sector. Ukraine that right now is standing in the beginning of the implementation process has to pay attention to the aspect of awareness due to various factor that currently causing low citizens' trust level to government that explicitly affects adaptation, acceptability and the eventual success of the eID project. The analysis of primary data that was gathered during the survey and interview conduction revealed quite a low level of Ukrainian citizens' awareness on e-governance, e-identification and, moreover, distrust to authorities. Seeking to tackle this matter, outlining a separate set of goals that focus on the awareness component and its inducement that consist of complex measures related to multiple levels and aspects of e-services provision to citizens and their utilization is required.

References

1. Aichholzer, G., Strauß, S.: The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity Inf. Soc. **3**(1), 65–85 (2010)
2. Al, A.A.R.A.: Citizens' perceptions towards e-governance: field study. World Acad. Sci. Eng. Technol. Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng. **7**(9), 2576–2584 (2013)
3. Al-Jaghoub, S., Al-Yaseen, H., Al-Hourani, M.: Evaluation of awareness and acceptability of using e-government services in developing countries: the case of Jordan. Electron. J. Inf. Syst. Eval. **13**(1), 1–8 (2010)
4. Arora, S.: National e-ID card schemes: a European overview. Inf. Secur. Techn. Rep. **13**(2), 46–53 (2008)
5. Draheim, D., Koosapoeg, K., Lauk, M., Pappel, I., Pappel, I., Tepandi, J.: The design of the estonian governmental document exchange classification framework. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2016. LNCS, vol. 9831, pp. 33–47. Springer, Cham (2016). doi:10.1007/978-3-319-44159-7_3

6. OECD: Digital Identity Management and Electronic Authentication. OECD (2011)
7. European Union: 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 (eIDAS Regulation). European Union (2014)
8. Grönlund, Å.: Electronic identity management in Sweden: governance of a market approach. Identity Inf. Soc. **3**(1), 195–211 (2010)
9. Hansteen, K., Ølnes, J., Alvik, T.: Nordic Digital Identification (eID), 1st edn, pp. 23–26. Nordic Council of Ministers, Copenhagen (2016)
10. Pappel, I., Pappel, I., Saarmann, M.: Digital records keeping to information governance in estonian local governments. In: Shoniregun, C.A., Akmayeva, G.A. (eds.) i-Society 2012 Proceedings: i-Society 2012, June 25–28, 2012, London, UK, pp. 199−204. IEEE, London (2012)
11. Pappel, I., Pappel, I.: Implementation of service-based e-government and establishment of state IT components interoperability at local authorities. In: The 3rd IEEE International Conference on Advanced Computer Control (ICACC 2011), Harbin, Hiina, 18–20.01.2011, pp. 371–378. Institute of Electronics and Computer Science, Singapore (2011)
12. Martens, T.: Electronic identity management in Estonia between market and state governance. Identity Inf. Soc. **3**(1), 213–233 (2010)
13. Potiy, A., Gorbenko, A., Korneyko, A., Kozlov, Y., Pushkarev, Y., Gorbenko, I.: EIDAS: principles of providing confidence electronic services and interoperability problem. Appl. Radio Electron. **13**(3), 252–260 (2014)
14. Sathe, V.: Managing massive change: India's aadhaar, the world's most ambitious ID project (Innovations Case Narrative: Project Aadhaar). Innovations Technol. Governance Globalization **9**(1–2), 85–111 (2014)
15. Sharma, V.: Aadhaar-a unique identification number: opportunities and challenges ahead. Res. Cell Int. J. Eng. Sci. **4**(2), 169–176 (2011)
16. Zhuzha, L.: Convert civil society in Ukraine thanks to the revolution of dignity. Int. Sci. J. **6**(1), 41–45 (2015)
17. State Migration Service of Ukraine: Запроваджено оформлення ID-паспортів для дорослих [Processing of ID-passports for adults has been implemented]. http://dmsu.gov.ua/component/content/article/9-ukrainska/novyny/novyny-dms-ukrainy/5041-zaprovadzheno-oformlennya-id-pasportiv-dlya-doroslikh. Accessed 30 Apr 2017
18. Львівська міська рада.: Картка львів'янина—учасника антитерористичної операції [Lviv Citizen card – the member of anti-terroristic operation]. http://city-adm.lviv.ua/services/card. Accessed 30 Apr 2017
19. ВолиньPost: Основні факти про заміну паперових паспортів на ID-картки [General facts about paper passport replacement with ID-cards]. http://www.volynpost.com/news/62294-osnovni-fakty-pro-zaminu-paperovyh-pasportiv-na-id-kartky. Accessed 03 May 2017

Appendix 2

II

V. Tsap. e-Identity and eIDAS: Interpretation of concepts by different countries. In A.-M. Osula and O. Maennel, editors, *Proceedings of ICR'2018 – the 4th Interdisciplinary Cyber Research Workshop 2018*, pages 9–10. Tallinn University of Technology, Department of Software Science, 2018. [last accessed 5 Nov 2021]
https://haldus.taltech.ee/sites/default/files/2021-04/ICR2018_proceedings.pdf

E-IDENTITY AND eIDAS: INTERPRETATION OF CONCEPTS BY DIFFERENT COUNTRIES*

Valentyna Tsap
Tallinn University of Technology
valentyna.tsap@ttu.ee

Background and previous work: Electronic identity is the prerequisite of today's e-government. Identity Management (IdM) has recently been under close attention of stakeholders, especially in the light of the eIDAS regulation that had come into force. So far, every national IdM system has been designed in accordance to its needs and strategy. This independence in the approach of managing identities has led to a EU-wide fragmentation of eIDs, both with respect to implementation and the understanding and interpretation of the concept itself[1]. It is now a huge challenge for each member state to fulfill the regulation's requirements to assure trust, security and interoperability. As the deadline for member states to notify their national eID schemes is approaching, it creates an additional pressure due to variance in readiness. There are countries that have already notified their eID schemes while others are still far behind the track[2]. If we are to look into countries' schemes' details, we expect to discover a wide range of aspects as obstacles to compliance with the regulation, and, in general, strong IdM system. We assume that a deeper understanding of those hindering factors and their comparison could help us to understand digital identity from the perspective of the countries that handle it. Digital identity itself is based on trust, the core concept that eIDAS is built on. The need for this regulation in the first place affirms the change and importance of these two notions, however, the variety of practices that can be observed on the international level stands as an evidence of difference in perception of the notion. Naturally, this difference can easily be reasoned in terms of practical necessities that a state has. But the question is what is behind the logic that leads to realizing these necessities.

As a part of our work, the concept of digital identity in the aspect of trust and awareness was discussed in previous papers. More precisely, a case of Ukraine was presented by evaluating the level of citizens' awareness towards e-ID. The study has also revealed a significant level of distrust to government that in terms of analysis allowed us to confirm how important is this component when introducing e-identity solutions[3].

Another aspect related to the dissertation concerns handling potential security threats in IdM of Estonia and is presented in the overview of an incident case study which will also be published in September 2018 within 7th International Conference on Electronic Government and the Information Systems Perspective.

Objectives: Our research aims at exploring countries' national eID systems and their comparison in terms of eIDAS regulation and countries' efforts to comply with it. The diversity of national eID systems holds an opportunity to identify: a) what are the obstacles that inhibit the process of compliance with eIDAS b) how digital identity is perceived in different countries and c) how strong and mature is it in those states?

Methods: We plan to conduct expert interviews with high-level government officials, executives, policymakers, specialist and other stakeholders that are involved in this field. We will also use other data collection techniques such as documentary evidence.

[*] Please note that this abstract has not gone through the double-blind peer review

Since in the literature, there is a rather little knowledge on IdM in a non-technical aspect, and also few definitions of the phenomenon of trust, the interviews, most probably, the interviews are going to be unstructured which will allow us to capture a wider range of data.

Within our research, we will cover at least 5 to 7 countries which will be chosen based on the geographical location and technological development criteria. Furthermore, there will be composed a comparative analysis of gathered data.

Expected results: We aim at making a contribution to a broader understanding of digital identity, in particular, how its concept is being changed in the light of ambitious efforts to build a large-scale environment where common and mutual trust is reached. There is a potential to find new general as well as personalized solutions to enhance and improve these systems. Our proposal is to approach the problem by trying to understand fundamental and seemingly obvious to everyone concepts more thoroughly.

Next Steps: Within the research, this topic will be presented and further developed at a round table on 18th European Conference on Digital Government in September 2018 in Santiago de Compostela, Spain.

Keywords: e-identity, e-government, eIDAS

REFERENCES

1. Seltsikas, P. and O'keefe, R.M., 2010. Expectations and outcomes in electronic identity management: the role of trust and public value. *European Journal of Information Systems*, 19(1), pp.93–103.
2. eIDAS implementation chart: up-to-date regulation in each country (6 Apr, 2017). EU Commission. Retrieved May 2018 from https://ec.europa.eu/futurium/en/content/eidas-implementation-chart-date-regulation-each-country
3. Tsap, V., Pappel, I. and Draheim, D., 2017, November. Key Success Factors in Introducing National e-Identification Systems. In International Conference on Future Data and Security Engineering (pp. 455–471). Springer, Cham.

Appendix 3

III

V. Tsap, I. Pappel, and D. Draheim. Factors affecting e-ID public acceptance: A literature review. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2019 – the 8th International Conference on Electronic Government and the Information Systems Perspective*, pages 176–188, Cham, 2019. Springer

Factors Affecting e-ID Public Acceptance: A Literature Review

Valentyna Tsap(✉), Ingrid Pappel, and Dirk Draheim

Information Systems Group, Tallinn University of Technology,
Akadeemia tee 15A, 12169 Tallinn, Estonia
{valentyna.tsap, ingrid.pappel,
dirk.draheim}@taltech.ee

Abstract. This paper presents a literature review that has the main goal to examine what are the factors that are affecting eID public acceptance. We are specifically interested in the perspectives of end-users and the matter of their attitudes towards eID. Our search yielded a rather narrow but concrete range of sources. Among the main themes of interest presented in the literature, we identify factors that are further synthesized in twelve categories. Moreover, we interpret the factors in their original context which allows for understanding which of the factors are mentioned as either drivers, barriers, or both. Based on the analysis of scientific narratives, we point to disparities detected in the existing knowledge of influential factors of eID public acceptance and outline areas that require further research.

Keywords: eID · Public acceptance · Literature review

1 Introduction

Electronic identity is a means to prove that you are the one that you claim to be online and thus granting access to e-services [17]. All over the world, governments have introduced national electronic identity schemes as a part of identity management. Electronic identity plays a vital role in the functioning of digital government infrastructure.

Considering countries' experience of introducing electronic government, it has been realized that for the success of such large-scale systems, the mere implementation of a technologically elegant solution is not sufficient. The importance of end-user acceptance cannot be overlooked. There is currently a struggle taking place when designing e-identity scheme that lies in the attempt of balancing the security of the solution and its usability. Even though, today, there are numerous successful practices, this does not guarantee the applicability and portability of those lessons learned. What works in one country, may not work in another.

As to date, there is no comprehensive study of factors that influence the user acceptance of national eID conducted. Thereby, the current research is exploratory.

A study [10], for instance, explores the aspect of acceptance of electronic identification system as a cross-border interoperability solution by all stakeholders and end-users. Another example can be a study where the focus is also set on the acceptance

A. Kő et al. (Eds.): EGOVIS 2019, LNCS 11709, pp. 176–188, 2019.
https://doi.org/10.1007/978-3-030-27523-5_13

factors of using in this case mobile identification applications [1]. An extent of research [3, 5, 20, 24, 38] focuses on theoretical background of the notion of technological acceptance.

Similar sources are considered within this review in order to present a broader and in-depth perspective on the possible influences of eID.

Hence, the main research question of this review is the following:

RQ: What Are the Factors That Affect eID Public Acceptance?
The intention is to analyze the existing literature in order to gather information about what is known about the particular issue of end users' acceptance of electronic identity that is moderated by the state. The intention is to conduct a search of primary sources and identify the key issues raised by theorists, practitioners, experts, adopters and other stakeholders involved in digital identity domain. We are particularly interested in exploring the studies that focus on the citizens' perspective of eID.

Semantic analysis of the existing literature will be performed to extract knowledge regarding digital identity in the named context. The extracted data will be then distributed to "drivers" and "barriers" categories as per the research question.

With this research, we strive to identify and point to the gap in the existing knowledge in order to spur future research with regards to eID public acceptance. Potentially, the derived results may be applied in building hypotheses and theories, as well as frameworks and evaluations.

2 Method

According to the literature review conduction guidelines [11, 34], the following steps were taken:

1. Identifying the need for literature review.
2. Formulation the research question.
3. Developing a search strategy.
4. Carrying out a comprehensive search of studies.
5. Analyzing and extracting data from the selected studies.
6. Synthesizing the results
7. Writing-up an interpretation of results.

Search Terms. The research question contains the following keywords: "factors, eID, user acceptance."

A list of synonyms for each of the keywords was constructed in order to increase the accuracy of search results. Moreover, the synonyms were selected based on the terms that are common to the researched area (e.g. "user" – "citizen"; "user acceptance" – "public acceptance"). The search terms were adapted to each of the resources searched as not all of them from the list enabled the use of Boolean operators and/or nesting.

Keywords ((*e-ID* OR *"electronic identity"* OR *"digital identity"* OR *"national e-ID" OR "national eID" OR*) AND (*barrier* OR obstacle* OR driver** OR *factor** OR *determinant** OR *influence** OR *impact* OR affect**) AND (*"user acceptance"* OR *"public acceptance"* OR *"citizen acceptance"* OR *perception** OR *attitude** OR *"user perception"* OR *"citizen perception" use* OR *usage*)).

Resources Searched. Using the keywords above, the following databases were searched:

- Google Scholar
- Scopus
- ACM Digital Library
- ScienceDirect
- Web of Science
- Springer Link
- IEEE Explore
- Digital Government Reference Library

To increase the number of found materials that fit the search criteria, the keywords were used in a direct search in the key journals and conference proceeding of the area. Additionally, each fitting item's reference list was scanned through for containing possible relevant materials.

Document Selection. The document selection is based on the following inclusion and exclusion criteria:

Authors include studies that:

- directly answer the research question;
- specifically focus on eID and not just e-government;
- mention the issue of acceptance of digital identity by citizens;
- based on empirical data;
- specifically mention societal aspects of technology acceptance of eID;

For this reason, within this study we will not be considering studies that do not provide any insight on the citizen perspective on eID.

Document Retrieval. The search has elicited 146 sources from databases. 88 of those were rejected based on the title and abstract analysis. The remaining sources were then evaluated based on the document selection criteria. The final revised list of selected papers is comprised of 39 items. Among the selected sources such types of documents were included to the review as conference proceedings, journal articles, book chapters, reports, policy documents, theses.

3 Results and Discussion

For the sake of clarification, it must be noted that though the search procedures applied within this study are very much resembling those used in systematic literature reviews (SLRs), we do not claim this review to be one of this kind. This review implements SLR guidelines only partially which is one of the reasons it does not qualify to be fully 'systematic'. As [10, 11] mark, SLR guidelines that originally have been applied in medicine, refer to the coverage of certain clearly identifiable evidence on specific medical treatments, while SLR guidelines outside medicine imply only the rigor of search process. Authors further point out that such limitation nowadays is more than often fails to be acknowledged. Like in SLRs, the upfront search inclusion/exclusion criteria have been introduced with the purpose of delineating and narrowing down the scope of the examined field according to our research aim. Only then, as what is usually done in traditional literature reviews (LRs), we build up criteria for interpreting the findings, i.e. identifying notions and further categorizing them.

The timeframe of selected studies captures the years of 2001–2018. This can be explained by the novelty of the subject of digital identity and its implementation worldwide.

The reviewed studies which outcomes derive from primary data represent country cases from around the globe though European region prevails.

Among 39 selected studies, 13 of them contain case studies with the data samples collected from one country each (Austria, Belgium, Canada, Estonia, Germany, Hong Kong, India, New Zealand, Switzerland, UAE, Ukraine, United Kingdom, USA;) among the rest 26 studies, findings in 17 of them are based on multiple countries data, and the 9 left represent findings of secondary data analysis. The data collected is derived mostly from the European continent which entails a predominantly Western perspective factors that influence eID public acceptance.

The items were selected on the basis of providing explicit insight about citizen perspective on eID. The papers in the final range differ by the extent of provided insight. While some papers had highlighted the eID acceptance by public rather incidentally focusing on other topics, the rest of the studies' aims were directly concerned the object of eID acceptance and the findings were based on primary and secondary data analysis. 9 studies included secondary data, while the rest 30 were presenting results of empirical data analysis.

The review of selected sources has allowed to extract the key notions mentioned by the authors that according to their hypotheses and findings determine the degree of eID public acceptance. The notions were extracted by means of semantic analysis of the selected sources. Categorizing the notions was also reasonable because of the number of synonymous notions that did not differ significantly in their meaning.

Another criterion for creating the categories and assigning their names was the frequency of notion occurring in the sources. For instance, the category of "trust" comprises detected notions concerning the issue of trust which are majorly referred to using the same value in most of the studies. This category also includes studies that mention the same phenomenon but referred to using synonymic notions. Such principle was applied throughout the entire process of categorization. It was decided to implement a condition that if the notion is mentioned less than in 10% of the studies, then it is going to be the category "Other".

The distribution of detected notions, i.e. any phenomenon authors mentioned to infer direct or indirect cause on the eID user acceptance, has allowed to create the following 12 categories: (1) complexity; (2) ease of use; (3) functionality; (4) awareness; (5) trust; (6) privacy concerns; (7) security; (8) control and empowerment; (9) transparency; (10) path dependency; (11) cultural and historical factors; (12) other.

The category "Other" will be further described separately as it contains miscellaneous notions that were not included in the former 11 ones.

Table 1 shows where and how frequently each notion is mentioned in the realm of selected papers.

Table 1. Table captions should be placed above the tables.

Category	Paper references
Complexity	[12, 15, 16, 22, 23, 29, 30, 41, 43]
Ease of use	[1, 3, 5, 6, 16, 20, 22, 24, 29, 31, 34–36, 39–41, 43, 44]
Functionality	[6, 15, 16, 18, 20, 22, 23, 25, 29, 31, 34, 35, 39, 41, 42, 45]
Awareness	[1, 2, 4, 14, 15, 18, 22, 23, 26–28, 31, 32, 34, 35, 39, 41–45]
Trust	[3–9, 12, 14–16, 18, 20, 21, 24, 26, 28, 29, 31–34, 36, 39–45, 48]
Privacy concerns	[1, 3, 5, 7–9, 15, 18, 20–22, 24–26, 30, 32, 34, 36, 39–46, 48]
Security	[1, 5, 7–9, 14, 15, 18, 21, 23, 24, 28, 32, 34, 40–44, 48]
Control and empowerment	[7–9, 12, 16, 18, 26, 27, 41–44, 46, 48]
Transparency	[7–9, 27–31, 33, 42, 43, 45]
Path dependency	[12, 20, 28, 33–35, 40, 45]
Cultural and historical factors	[2, 12, 20, 27, 34, 42, 45]

A number of papers [1, 3–6, 12, 22, 26, 31, 35, 41, 43], studying the acceptance of eID, have incorporated TAM and its extensions [17, 47]. This had an impact on the design of the research by crafting the studies according to the elements of TAM [1, 3–6, 41] or rather providing guidance and serving as a background concept [12, 22, 31, 35, 43]. TAM has also influenced the derivation of notion categories in this review.

Ease of Use. This category echoes the element of TAM that has the same name. This category comprises such notions as “convenience” [1, 12, 15, 16, 24, 35, 42], “user friendliness” [6, 16, 30, 34, 39], “usability” [1, 6, 16, 22, 25, 43], “comfort” [18, 22]. For instance, Kalvet *et al.* uses the term “convenience” when referring to the physical appearance and properties of an eID card [24]. Such terms as “usability”. “usefulness”, “user friendliness” appear in studies that are having a TAM view within their methods.

Complexity. This category was distinguished despite the thought that it might contradict with the just mentioned notion of ease of use. However, this depends on one’s perspective where, for instance, the system that is seen to be complex due to lack of awareness, but on the other hand, can be named so even though another user can understand it regardless [15]. In [46], the term “complexity” is mentioned in the context of information systems and their structure. The issue of complexity in the survey from study [22] is referred as a difficult-to-understand mechanism of the system.

Functionality. This category includes notions that echo the “usefulness” element of TAM. These are the notions “usefulness” (importantly, without implying to TAM), availability of options (such as authentication methods or e-services available). For example, findings of [6] show that availability of services linked to eID is of importance when deciding whether using eID is useful for the citizens.

Awareness. The following category includes such expressions mentioned as "understanding" [15, 22], "seeing reasons/purpose" [30], "knowing how to use" [8], "comprehending". [8] indicates "awareness" in the context of knowing how the systems works and knowing how to use it and connects this notion to the trust. [44] suggests that awareness of, for instance, technical aspects of a currently implemented solution, will not guarantee the acceptance of future updates and changes, which implies the temporariness of this factor.

Control and Empowerment. The given category refers to "control over eID/e-identity/identity" [21], "empowerment of citizens" [2, 15, 16, 26], i.e. their ability to choose whether to use eID, which data to provide, ability to check the status of data, ability to withdraw data, participation. [15] mentions "empowerment" in the context of citizens being able "to access their information without "bureaucracy". In [2], authors use "empowerment" as a reference to access to services, more precisely "so that they can legally control service delivery to their advantage." In [21], "control" appeared as a major theme during analysis of primary data and concerned control of citizens over their personal data as well as the issue of data integrity and disclosure by consent.

Transparency. This category generalizes the understanding of underlying principles of how (accountable) the data is being handled in legal, administrative and procedural sense by authorities [26, 46]. [2] defines "transparency" as a result of a process of "bringing visibility to citizens of the service workflow by means of automated service delivery." The comparative study on citizen perceptions of eID and interoperability [21] provides a formulation of "transparency" given by a citizen as "ALL data that are collected about me should be made available to me, so that I am able to recognize who has collected what data about me." In [31], the context brings up "transparency" along with the approach organizations handle data with.

Path Dependency. This particular category that somewhat represents rather a different perspective than the citizen one, yet it was introduced due to the arguments in studies [12, 33] justifying the fact that paths chosen by countries and the previous setting they possess (including societal) when introducing eID are definitive for the perceptions of stakeholders (including end-users, i.e., citizens).

Path dependency refers to "previous technical, organizational and regulatory settings explain for the differences in the provisioning of national eID systems and thus the heterogeneous landscape of solutions and usage across Europe" [12]. Within our study, we define path dependency as rather an external factor of influence that has not been articulated by end-users within the sample of this review. [33] highlights the need of understanding the scenarios that worked out successfully in one country's case and did not prove itself when applying the same strategies in another country. Authors then state that citizens as one of the stakeholders have a major potential to determine the outcome of each scenario. Hence, they suggest to explore more deeply eID introduction in the socio-material perspective, i.e. citizens' relationships with eID artefacts.

Cultural and Historical Factors. 5 studies [1, 4, 12, 20, 31] have provided insights on the role of culture and history in shaping citizen perceptions and acceptance of eID. An elaborate opinion on how historical events can have a major impact and shape the sense of identity is given in the case study of the Hong Kong eID [20]. In the rest of the studies, history and culture are discussed more in general.

The categories of “privacy concerns”, “security” and “trust” are the most frequent within this study. The names of these categories were assigned according to the same notions identified during analysis. All three notions are seen as issues to be leveraged in order to increase their trustworthiness in the eyes of the citizens [12].

Privacy concerns. Notions related to this category are associated with risks, fears, threats to citizens’ rights to be violated in relation to their digital identities.

Security. Here, the identified notions are related to data, software, and hardware, their reliability, trustworthiness, safety, and the ability of state to provide this security.

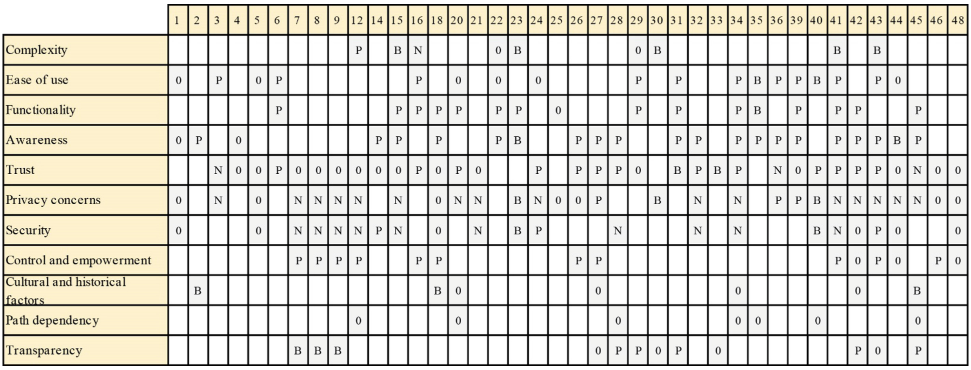
Trust. This category that is the most prevailing one. Even though we do not make any claims about the degree of influence that each identified factor has, trust has been seen and presented by researchers as one the most important pre-conditions of eID success. Trust is interrelated to most of the other categories and could be divided into subcategories or appear as a standalone factor. In [29], “trust” is displayed a two-type concept [48] that included institution-based trust and characteristic based trust. Here, the institution-based trust represents the trust that citizens experience towards public authorities and their activities, whereas characteristic-based trust is the one that end-users put in the system or solution. Another study [32] identifies ‘trust’ as well as ‘distrust’ as two independent and separate sides of the same relationship and not as two opposites of one continuum. These two sides, as authors explain, co-exist and evolve as the relationship matures and evolves over time. Here, term ‘relationship’ is used in the socio-technical and political context. Therefore, ambivalence is the main attribute and finding regarding trust and distrust that variates from country to country clearly influencing the development outcomes.

Other. This category includes notions that have not been assigned to the abovementioned categories. One of the notions is the ‘intrinsic motivation to adopt the technology’ (i.e. eID) [22]. The same source has identified cost and expenses associated with the use of eID as an influential factor as well as the extent to what the technology has to spread before the user will actually start adopting it him or herself. This tendency particularly echoes the diffusion of innovation theory where such users are known as Late Adopters [38]. Lastly, the survey conducted within the study [20] has also identified as an impact factor the citizens’ possibility to receive help from a competent person when using the technology, or in other words, technical support.

Going back, the issue of cost was raised also in [12]. Authors of [5] proposed a model with six key elements that affect the adoption of identity management systems, one of which – ‘individual differences’ – was distinguished as a notion in our research as well. The element of ‘individual differences’ is then divided in two sub-elements: demographic variables and situational variables that both have direct and moderating effects. The demographic differences include gender, age and education as characteristic of individuals and the situational ones are referred to as context-sensitive characteristics, i.e., experience, facilitating conditions, subjective norm and cost. A study on the acceptance of biometrics in identity management [24] revealed that “age, gender, education level and occupation do not influence the respondents’ views on the acceptability of biometric identity databases in any considerable way." In [33], authors mention such factors as eID user maturity and national differences in perceptions of information systems.

The derived categories can be potentially used as metrics for assessing the acceptance levels of eID. An attempt was made to interpret each identified notion as a driver or barrier of eID acceptance depending in what context it was mentioned. The identified notions were then marked as 'positive', 'negative', 'bilateral', or 'neutral'. In other words, a notion is presented as a driver or a barrier. Moreover, the impact of a notion may range and hereby it can be assigned to both positive and negative group. Lastly, some derived notions were not interpreted neither as positive nor as negative. Additionally, some studies elaborate on the notions in a neutral context by not inferring their positive or negative impact but merely assuming the possibility of impact.

Figure 1 represents the categories and their context in the sources they were extracted from. Depending on the context, a set of indicators was established where "**P**" is "**positive**", "**N**" is "**negative**", "**B**" is "**bilateral**" and "**0**" is "**neutral**". The headings of columns represent the reference numbers of studies that can be found in the References section.



	1	2	3	4	5	6	7	8	9	12	14	15	16	18	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	39	40	41	42	43	44	45	46	48
Complexity										P		B	N				0	B						0	B									B		B				
Ease of use	0		P		0	P							P		0		0		0					P		P			P	B	P	P	B	P		P	0			
Functionality						P						P	P	P	P		P	P		0				P		P			P	B		P		P	P			P		
Awareness	0	P		0							P	P		P			P	B			P	P	P			P	P		P	P	P	P		P	P	P	B	P		
Trust			N	0	0	P	0	0	0	0	0	0	P	0	P	0			P		P	P	P	0		B	P	B	P		N	0	P	P	P	P	0	N	0	0
Privacy concerns	0		N		0		N	N	N	N		N		0	N	N		B	N	0	0	P			B		N		N		P	P	B	N	N	N	N	N	0	0
Security	0				0		N	N	N	N	P	N		0		N		B	P				N				N		N				B	N	0	P	0			0
Control and empowerment							P	P	P	P			P	P							P	P												P	0	P	0		P	0
Cultural and historical factors		B												B	0							0							0						0			B		
Path dependency										0					0								0						0	0			0					0		
Transparency							B	B	B													0	P	P	0	P		0							P	0		P		

Fig. 1. Derived categories.

4 Limitations

Completeness. The search conducted within this review has elicited a fairly small amount of literature. As the aim of the review was to identify factors that specifically influence public acceptance of eID and not any other component of e-government, it explains the low number of included studies. However, the document selection criteria and search query design allowed for targeting papers which content accurately addresses the issue of eID public acceptance. There were no limitations set regarding the inclusion or exclusion of a particular document type but mostly academic sources appeared in the search results. Further inclusion of policy papers, white papers, and grey literature will be considered when broadening the scope of this research.

Potential Bias. The presented review is conducted within a research for doctoral thesis and hence the likelihood of results influenced by the bias of authors is high. This calls for further validation and assessment of the results by involving other researchers. As the studies in the range of review are mostly displaying findings from data gathered among European countries, generalization is possible only to some extent. As to the process of interpreting and deriving the categories, there is an inevitable effect of subjectivity. To lower this effect, a consensus has to be reached on the basis of a previous review that comes from independent researchers.

Data Synthesis. The findings of papers were analyzed to answer the research question allowing to identify the occurring notions and categorizing them. It is suggested that while grouping them it may have been possible that some of the notions where aggregated into wrong categories as well as there is chance that there could have been created a bigger or smaller number of categories. This serves as an additional motivation to iterate the analysis extending the study.

Future Research. As the eID user acceptance can be viewed from various perspectives, it is more than necessary to extent the study. We consider an attempt to segregate the existing results with those the perspectives on eID public acceptance of other stakeholders. Some papers that were analyzed within this review already provide other stakeholders' perspectives, however, due to the focus of this study, these insights were not considered. The study will benefit if the acceptance factors will be compared and analyzed along with those define the acceptance of similar or larger ISs. A great realm of research and analysis that looks into e-government acceptance as a whole offers much richer outcomes on the subject. As we noted before, it is realized that the derived notions overlap with ones that are also definitive in the case of e-government acceptance, there a still factors that are specific to eID which have to be investigated further.

The prevailing majority of the studies in this review highlighted the issue of trust and privacy concerns which calls for a more detailed analysis of these categories. Even though the goal within this review was to identify factors of impact and through the course of data synthesis and interpretation, each distinguished category was given the same value and weight, the authors of included studies insist on the importance of these notions. Therefore, we also support the idea of this direction to be explored more thoroughly.

The analysis of the studies confirmed that at the moment the body of knowledge contains a rather scarce and fragmented picture of what is of importance for public acceptance of eID especially from citizens' perspective.

5 Conclusion

The findings suggest the eID public acceptance to be a multifaceted phenomenon that is influenced by a wide range of variables with a different degree of impact. The studies with the empirical data analysis provide a sufficient basis only for a primary conceptualization.

Overall, the number of studies elicited by the given criteria leads points to a knowledge gap in the understanding and interpretation of eID public acceptance from citizens' perspective.

While deriving the categories, it has been realized how strongly interconnected these variables are and, in some cases, can imply very similar if not identical or, conversely, ambiguous facts or assumptions. The analysis allowed to construct a list with 12 categories that consist of identified factors influencing eID public acceptance. Composing the list of categories also shed light on a trend among researchers to focus on the issues of trust, privacy and security when it comes to user acceptance of eID. Though a relatively significant body of knowledge on these issues exists, it is encouraged to proceed with going further, especially taking the societal angle. Since derived categories are heavily dependent on each other and hence it is a challenge to establish what is a primary cause for what, needless to point out that this cause-effect relationship varies from country to country.

It is clear that some factors identified, for instance, history, culture and path dependency deserve more attention due to little knowledge about their role in defining citizens' perceptions of eID. This fraction of research would be also interesting to conduct considering the shifts in the notion of identity itself.

Of course, the derived factors and categories are echoing factors that determine the acceptance of e-government services in general. The consistency of our findings with previous research is obvious however the identified gaps evidently call for further research in this particular stream, i.e. eID public acceptance factors.

References

1. Ahrenstedt, S., Huang, J., Wollny, L.: A study on factors influencing the acceptance of mobile payment applications in Sweden. Dissertation (2015). http://urn.kb.se/resolve?urn=urn:nbn:se:hj:diva-26738
2. Al-Hujran, O., Al-dalahmeh, M., Aloudat, A.: The role of national culture on citizen adoption of eGovernment services: an empirical study. Electron. J. E-Government **9**(2), 93–106 (2011)
3. Alkhalifah, A., Al Amro S.: Understanding the effect of privacy concerns on user adoption of identity management systems. J. Comput. **12**(2), 174–182 (2017). https://doi.org/10.17706/jcp.12.2.174-182
4. Alkhalifah, A., D'Ambra, J.: The role of trust in the initial adoption of identity management systems. In: Linger, H., Fisher, J., Barnden, A., Barry, C., Lang, M., Schneider, C. (eds.) Proceedings of the 2012 International Conference on Information Systems Development, pp. 25–39. Springer, Heidelberg (2013). https://doi.org/10.1007/978-1-4614-7540-8_27
5. Alkhalifah, A.: Factors effecting user adoption of identity management systems: an empirical study (2012)
6. Andermatt, K.C., Göldi, R.A.: Introducing an electronic identity: the co-design approach in the canton of schaffhausen. Schaffhausen Swiss Yearb. Adm. Sci. **9**, 41–50 (2018). https://doi.org/10.5334/ssas.122
7. Backhouse, J., Halperin, R.: A survey on EU citizens trust in ID systems and authorities (2007)

8. Backhouse, J., Halperin, R.: Approaching interoperability for identity management systems. In: Rannenberg, K., Royer, D., Deuker, A. (eds.) The Future of Identity in the Information Society, pp. 245–268. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01820-6_6
9. Backhouse, J., Halperin, R.: Security and privacy perceptions of e- ID: a grounded research. In: Proceeding of the 16th European Conference on Information Systems, ECIS 2008, Galway, Ireland (2008)
10. Boell, S.K., Cecez-Kecmanovic, D.: On being "systematic" in literature reviews in IS. J. Inf. Technol. **30**(2), 161–173 (2015)
11. vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., Cleven, A.: Standing on the shoulders of giants: challenges and recommendations of literature search in information systems research. Commun. Assoc. Inf. Syst. **37**(1), 205–224 (2015)
12. Brugger, J., Fraefel, M., Riedl, R.: Raising acceptance of cross-border eID federation by value alignment. Electron. J. e-Government **12**(2), 178–188 (2014)
13. Budgen, D., Brereton, P.: Performing systematic literature reviews in software engineering. In: Proceedings of the 28th International Conference on Software Engineering, pp. 1051–1052. ACM, May 2006
14. Cap, C.H., Maibaum, N.: Digital identity and its implications for electronic government. In: Schmid, B., Stanoevska-Slabeva, K., Tschammer, V. (eds.) Towards the E-Society - E-Commerce, E-Business, and E-Government; (I3E'01), Zürich, pp. 803–816 (2001)
15. Chauhan, S., Kaushik, A.: Evaluating citizen acceptance of unique identification number in India: an empirical study. Electron. Gov. Int. J. **12**(3) (2016). https://doi.org/10.1504/eg.2016.078416
16. Cuijpers, C., Schroers, J.: eIDAS as Guideline for the Development of a Pan-European eID Framework in FutureID. GI-Edition Lect Notes Informatics (2015)
17. Davis, F.D.: A technology acceptance model for empirically testing new end-user information systems: theory and results. Doctoral dissertation, Massachusetts Institute of Technology (1985)
18. European Commission. Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union (2011)
19. European Commission. Electronic Identities - A brief introduction 6 (2015). http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf
20. Goodstadt, L.F., Connolly, R., Bannister, F.: The Hong Kong e-Identity card: examining the reasons for its success when other cards continue to struggle. Inf. Syst. Manag. **32**(1), 72–80 (2015). https://doi.org/10.1080/10580530.2015.983025
21. Halperin, R., Backhouse, J.: A Qualitative Comparative Analysis of Citizens' Perception of EIDs and Interoperability (2008)
22. Harbach, M., Fahl, S., Rieger, M., Smith, M.: On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In: De Cristofaro, E., Wright, M. (eds.) PETS 2013. LNCS, vol. 7981. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-39077-7_13
23. Jones, L.A., Antón, A.I., Earp, J.B.: Towards understanding user perceptions of authentication technologies. In: Proceedings of 2007 ACM Workshop on Privacy in Electronic Society (WPES 2007), pp. 91–98 (2007). https://doi.org/10.1145/1314333.1314352
24. Kalvet, T., Tiits, M., Laas-Mikko, K.: Public acceptance of advanced identity documents. In: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance – ICEGOV 2018, pp. 429–432. ACM Press, New York (2018)
25. Khan, H., Hutchison, A.: Data privacy implications for security information and event management systems and other meta-systems. In: Felici, M. (ed.) CSP 2013. CCIS, vol. 182 (2013). https://doi.org/10.1007/978-3-642-41205-9_7

26. Adjei, J.K.: A Case for Implementation of Citizen Centric National Identity Management Systems: Crafting a Trusted National Identity Management Policy, 1 edn. Institut for Elektroniske Systemer, Aalborg Universitet (2013)
27. Lips, M.: Rethinking citizen-government relationships in the age of digital identity: insights from research. Inf. Polity **15**(4), 273–289. https://doi.org/10.3233/ip-2010-0216
28. Lips, S., Pappel, I., Tsap, V., Draheim, D.: Key factors in coping with large-scale security vulnerabilities in the EID field. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2018. LNCS, vol. 11032, pp. 60–70 (2018). https://doi.org/10.1007/978-3-319-98349-3_5
29. Lockton, V.M.: e-Government and Identity Management in British Columbia: Implementation of the BCeID (2009)
30. Mariën, I., Van Audenhove, L.: The Belgian e-ID and its complex path to implementation and innovational change. Identity Inf. Soc. **3**(1), 27–41 (2010). https://doi.org/10.1007/s12394-010-0042-2
31. Marzooqi, S.A., Nuaimi, E.A., Qirim, N.A.: E-governance (G2C) in the public sector: citizens acceptance to E-government systems - Dubai's case. In: Proceedings of the Second International Conference on Internet of Things, Data and Cloud, ICC 2017. https://doi.org/10.1145/3018896.3025160
32. McGrath, K.: Identity verification and societal challenges: explaining the gap between service provision and development outcomes. MIS Q. **40**, 485–500 (2016). https://doi.org/10.25300/misq/2016/40.2.12
33. Melin, U., Axelsson, K.: Managing the development of e-ID in a public e-service context: challenges and path dependencies from a life-cycle perspective. Transf. Gov.: People Process Policy **7**(2), 240–255 (2013). https://doi.org/10.1108/TG-08-2013-0026
34. Ng-kruelle, G., Swatman, P.A., Hampe, J.F., Rebne, D.S.: Biometrics and e-Identity (e-Passport) in the European union : end-user perspectives on the adoption of a controversial innovation. J. Theoret. Appl. Electron. Commerce Res. **1**(2), 12–35
35. Palgin, M.-L.: Diffusion of the estonian ID-card and its electronic usage: explaining the success. Master's thesis, Tallinn University of Technology (2016)
36. Perakslis, C., Wolk, R.: Social acceptance of RFID as a biometric security method. IEEE Technol. Soc. Mag. **25**, 34–42 (2006)
37. Petticrew, M., Roberts, H.: Systematic Reviews in the Social Sciences. Blackwell Publ, Malden (2012)
38. Rogers, E.M.: Diffusion of Innovations. Simon and Schuster, New York (2010)
39. Rossnagel, H., Camenisch, J., Fritsch, L., et al.: FutureID - shaping the future of electronic identity. Datenschutz und Datensicherheit **36**, 189–194 (2012)
40. Seltsikas, P., O'Keefe, R.M.: Expectations and outcomes in electronic identity management: the role of trust and public value. Eur. J. Inf. Syst. **19**(1), 93–103 (2009). https://doi.org/10.1057/ejis.2009.51
41. Seven, A.: Building sustainability and trust in the usage of electronic identification using technology acceptance model. Doctoral Dissertation, Juame I University (2015)
42. Snijder, M.: Security & Privacy in Large Scale Biometric Systems. Special Eurobarometer, p. 359 (2006)
43. Strauß, S., Aichholzer, G.: National electronic identity management: the challenge of a citizen-centric approach beyond technical design. Int. J. Adv. Intell. Syst. **3**(1), 12–23 (2010)
44. Tiits, M., Kalvet, T., Laas-Mikko, K.: Social acceptance of ePassports. In: Proceedings of the 13th International Conference of the Biometrics Special Interest Group, 10–12 September 2014, Darmstadt, Germany. LNI, pp. 15–26 (2014)

45. Tsap, V., Pappel, I., Draheim, D.: Key success factors in introducing national e-Identification systems. In: Dang, T., Wagner, R., Küng, J., Thoai, N., Takizawa, M., Neuhold, E. (eds.) FDSE 2017. LNCS, vol. 10646, pp. 455–471. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70004-5_33
46. van Rooy, D., Bus, J.: Trust and privacy in the future internet – a research perspective. Identity Inf. Soc. **3**(2), 397–404 (2010). https://doi.org/10.1007/s12394-010-0058-7
47. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**, 425–478 (2003)
48. Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M.: Encouraging citizen adoption of e-government by building trust. Electron. Markets **12**(3), 157–162 (2002). https://doi.org/10.1080/101967802320245929

Appendix 4

IV

V. Tsap, S. Lips, and D. Draheim. eID public acceptance in Estonia: towards understanding the citizen. In S.-J. Eom and J. Lee, editors, *Proceedings of dg.o'20 – the 21st Annual International Conference on Digital Government Research: Intelligent Government in the Intelligent Information Society*, pages 340–341. Association for Computing Machinery, 2020

eID Public Acceptance in Estonia: towards Understanding the Citizen

Valentyna Tsap
valentyna.tsap@taltech.ee
Tallinn University of Technology
Tallinn, Estonia

Silvia Lips
silvia.lips@taltech.ee
Tallinn University of Technology
Tallinn, Estonia

Dirk Draheim
dirk.draheim@taltech.ee
Tallinn University of Technology
Tallinn, Estonia

ABSTRACT

Estonia eID is officially a part of the critical infrastructure. 2/3 of citizens regularly use eID today to access thousands of e-services. To examine the eID public acceptance, we conducted a survey among Estonian eID users to find out which of the existing eID authentication options are preferred and why. We present the results and interpret the data with a set of pre-defined eID public acceptance factors.

CCS CONCEPTS

• **Applied computing** → **E-government**; • **Security and privacy** → *Authentication*; Social aspects of security and privacy; • **Social and professional topics** → Socio-technical systems.

KEYWORDS

eID, authentication, Estonia, public acceptance

ACM Reference Format:
Valentyna Tsap, Silvia Lips, and Dirk Draheim. 2020. eID Public Acceptance in Estonia: towards Understanding the Citizen. In *The 21st Annual International Conference on Digital Government Research (dg.o '20), June 15–19, 2020, Seoul, Republic of Korea.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3396956.3397009

1 INTRODUCTION

Identity management has been one of the crucial building blocks of e-government and electronic service provision. The current heterogeneity among the EU states' e-governance initiatives has become a hindering factor in the movement towards cross-border interoperability and digital single market. In recent years, fundamental changes have been introduced into policies, regulations and legislation on the international level to assure a common path for everyone (e.g. eIDAS Regulation).

e-Government and e-service provision rely on identity management. Today, within EU, heterogenous eID systems became an obstacle to the way of creating the digital single market and cross-border interoperability. The states work hard by bringing changes into policies, laws on international level to ensure a common path to achieving this goal. Despite a huge amount of sources contains knowledge and practices related to identity management, gaps still do exist [Buldas et al. 2018]. The research on eID provides a decent amount of information on on the technological aspects (e.g. architecture, cryptography) privacy, security, policy (e.g. implementation and adoption). Whether these are studied separately or combined, the amount of citizen-oriented research in this domain remains to be smaller [Al-Hujran et al. 2011; Chauhan and Kaushik 2016].

Table 1: eID acceptance factors

Factor	**Interpretation**
Complexity	How citizens (subjectively) see and perceive the application/tool related to computer and digital literacy;
Ease of use	Convenience and amount of effort during the use, usability;
Functionality	Number and range of options the application/tool offers, usefulness;
Awareness	How well citizens are informed about the application/tool, its availability, purpose, provider, etc.
Trust	Feeling of trust towards the application/tool and its creator/provider;
Privacy	Risks, fears, threats to digital identities citizens have;
Security	Issues on data, software, and hardware, their reliability, trustworthiness, safety, and the ability of state to provide this security perceived by citizens;
Control and empowerment	Availability of options to use/view/control/edit/delete/withdraw one's data;
Transparency	How the visibility and accountability on how personal data is handled and service provision is delivered to citizens

In Estonia, eID is an essential component of the e-government ecosystem [Pappel et al. 2017]. It is an element of the X-Road data exchange layer. eID is an enabler for accessing e-services and e-voting. e-Residency rests on the eID infrastructure [Kalja 2012; Tsap et al. 2017].

There are several authentication options available to Estonians. e-Services can be accessed by means of ID-card, digital identity card (only for authentication and digital signature), Mobile ID, Smart ID (a cloud-based solution), Bank ID, user name and password, PIN-calculator.

dg.o '20, June 15–19, 2020, Seoul, Republic of Korea

ACM ISBN 978-1-4503-8791-0/20/06.
https://doi.org/10.1145/3396956.3397009

Around two thirds of Estonian citizens use eID regularly[1]. This country serves as a case that is worth to be investigated exactly from citizen-end angle. Identifying users' preferences and attitudes can serve as a feedback to policy makers, service providers and other parties of the identity management domain [Gupta et al. 2012]. Changing perspective, we will examine the existing gap by studying the drivers of eID acceptance in the settings of Estonia. Being aware of the state's history and path of eID implementation, we will look at citizens' perceptions and find out their preferences regarding the available eID authentication options and factors contributing to their acceptance.

Therefore, we created a survey for Estonian eID owners and investigate motivations, reasons, and aspects of using eID. As there are several eID solutions offered to citizens, we include all of them in the survey, in order to acquire a more in-depth insight. To analyse the results, we use factor of eID public acceptance derived from our prior research [Tsap et al. 2019]. Moreover, we add to the analysis statistical data on different eID means provided by the Estonian trust service provider for more detailed and accurate results.

We used case study research with a survey with multiple-answer and open-ended questions to collect our data. In total, we have received 268 responses.

In Table 1, the factors are briefly summarized based on their full description in the previous research to give an understanding of our findings [Tsap et al. 2019].

According to the results of our survey, about 82% of respondents use ID card, 65% - Smart ID, 46% - Mobile ID, 37% - Bank links, less than 10% use other options, for example, ones provided by employers, PIN-calculators.

The respondents were asked to explain their choices and share their thoughts on the available authentication options. We have summarized their responses, analysed them and created an additional tagging system to group these responses. Table 2 shows which features and which combinations of features were mentioned. Based on the frequency, we distinguished three features such as Convenience, Security, Speed to see the total numbers clearer. Each of these features contribute to the "ease of use" factor. Within this particular range of answers, respondents have also mentioned authentication options they prefer the most. The most frequently mentioned was Smart ID, then Mobile ID, and, lastly, ID card.

The PKI authority of Estonia has also provided data on the use of Mobile ID and Smart ID. The numbers suggest that since the launch of Smart ID, its popularity and use has grown significantly, and less than in five months, outran Mobile ID.

The citizens were also asked do they trust service providers when their personal data is processed. 20% responded they have full trust; same amount replied they do trust but not without some concerns; about 36& felt skeptical about it, around 6% do not trust the service providers. In general, these number are rather positive and favourable towards the state.

To conclude, the received outcomes do not suggest there is a consensus on particular features of eID that make them ultimately appealing and universally best for all citizens. The choice will always depend on circumstances, hardware, purpose, services accessed, trust. The range of available authentication options may somehow be optimal since there is not one, but at least three and more options that citizens use regularly.

Table 2: Response summary.

Features	Mention	Percentage
Convenience	41	18
Convenience + Security	17	6
Convenience + Speed	27	10
Convenience + Speed + Security	7	3
Ease of use	10	4
Security	8	6
Speed + Security	5	2
Speed	16	6
Usability	2	1
No additional device needed	5	2
Availability	5	2
Convenience in total	101	38
Security in total	38	14
Speed in total	65	25

Estonia sure does serve a valuable lesson and experience which could be useful to others. We point to the need to explore the aspects of citizens' preferences even further to gain knowledge the "ease of use" factor of eID and others that has been outlined by the analysis. A continued study will be required to examine the Estonian eID from the perspective of other public acceptance factors.

REFERENCES

O Al-Hujran, M Al-dalahmeh, and A Aloudat. 2011. The Role of National Culture on Citizen Adoption of eGovernment Services: An Empirical Study. *Electronic Journal of e-Government* 9, 2 (2011), 93–106.

Ahto Buldas, Martha Jung, Kaja Kuivjõgi, Anna-Maria Osula, Rain Ottis, Jaan Priisalu, Liisa Tallinn, and Toomas Vaks. 2018. *ID-kaardi kaasuse õppetunnid.* Technical Report. Tallinn University of Technology , School of Information Technologies, Department of Software Science, Tallinn, Estonia.

Sumedha Chauhan and Anjali Kaushik. 2016. Evaluating Citizen Acceptance of Unique Identification Number in India: an Empirical Study. *Electronic Government, an International Journal* 12, 3 (2016), 223–242. https://doi.org/10.1504/EG.2016.078416

Nidhi Gupta, Arnout R.H. Fischer, and Lynn J. Frewer. 2012. Socio-psychological determinants of public acceptance of technologies: A review. *Public Understanding of Science* 21, 7 (2012), 782–795. https://doi.org/10.1177/0963662510392485

Ahto Kalja. 2012. The first ten years of X-Road. *Estonian Information Society Yearbook 2011/2012* (2012), 78–80.

Ingrid Pappel, Ingmar Pappel, Jaak Tepandi, and Dirk Draheim. 2017. Systematic digital signing in Estonian e-Government processes: Influencing factors, technologies, change management. In *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI,* Thoai N. Hameurlain A., Küng J., Wagner R., Dang T. (Ed.). Vol. 10720 LNCS. Springer, Berlin, Heidelberg, 31–51. https://doi.org/10.1007/978-3-662-56266-6_2

Valentyna Tsap, Ingrid Pappel, and Dirk Draheim. 2017. Key Success Factors in Introducing National e-Identification Systems. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* T.K. Dang (Ed.), Vol. 10646 LNCS. Springer, Cham, Ho Chi Mihn City, Vietnam, 455–471. https://doi.org/10.1007/978-3-319-70004-5_33

Valentyna Tsap, Ingrid Pappel, and Dirk Draheim. 2019. Factors Affecting e-ID Public Acceptance: A Literature Review. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* Vol. 11709 LNCS. Springer International Publishing, 176–188. https://doi.org/10.1007/978-3-030-27523-5_13

[1] https://www.id.ee/?lang=en

Appendix 5

V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2020 – the 9th International Conference on Electronic Government and the Infor-mation Systems Perspective*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer

Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia

Valentyna Tsap( ), Silvia Lips, and Dirk Draheim

Tallinn University of Technology, 12619 Tallinn, Estonia
{valentyna.tsap,silvia.lips, dirk.draheim}@taltech.ee

Abstract. Estonia is an advanced digital society where eID is considered as part of the critical infrastructure. With the current number of e-services that the state offers to citizens and businesses, more than 2/3 of citizens regularly use eID today. We investigate the reasons that stand behind its public acceptance. We have conducted a survey among Estonian eID users with 268 respondents to find out which of the existing eID authentication methods are preferred the most (smart cards, Mobile ID, cloud-based solutions, bank links, usernames and passwords, etc.) and what are the decisive factors for these preferences. We have presented and discussed the results by interpreting the data with a set of pre-defined eID public acceptance factors. The outcomes suggest that users prioritize convenience, speed, and security as well as availability of co-existing multiple authentication methods that suit them depending on the setting and circumstances. Moreover, we explain the importance of other contributing factors specific to the case of Estonia.

Keywords: eID · Authentication · Estonia · Public acceptance

1 Introduction

Identity management has been one of the crucial building blocks of e-government and electronic service provision. The current heterogeneity among the EU states' e-governance initiatives has become a hindering factor in the movement towards cross-border interoperability and digital single market. In recent years, fundamental changes have been introduced into policies, regulations and legislation on the international level to assure a common path for everyone (e.g. eIDAS Regulation).

Though the regulations and normative documents have accumulated an exhaustive realm of knowledge and experience to improve electronic identity management, not all aspects have been sufficiently covered [8]. With respect to the subject of eID being present in the literature, so far it can be stated that there is a definite array of work that concentrates on the technological aspects (e.g. architecture, cryptography [19], privacy [3,26], security [4], etc.), policy

A. Kő et al. (Eds.): EGOVIS 2020, LNCS 12394, pp. 159–173, 2020.
https://doi.org/10.1007/978-3-030-58957-8_12

(e.g. implementation and adoption) [12], aspects on different scales [1,4]. While each of them were studied either in isolation or in conjunction with others, it has been noticed that the input to the citizen-oriented research is rather minor [2,9]. It is more common to come across literature that covers a broader angle on the acceptance of technology while we are interested in evidence on a specific aspect.

In Estonia, eID is a vital part of the e-government ecosystem [24]. It is a component of the X-Road data exchange layer. This way, eID enables access to e-services and e-voting. It also serves as the main infrastructure for e-residency [17,27,31].

Estonians have at their disposal several methods of authentication for accessing e-services such as ID-card, digital identity card (suitable only for authentication and digital signing), Mobile ID, Smart ID (cloud-based solution), Bank ID, user name and password, PIN-calculator, social media accounts. It is worth to note that due to the focus of this study, we do not cover the technical specifications of the abovementioned eID solutions.

Nowadays, two thirds of the Estonian population are using eID on a regular basis [16]. Thus, the country presents itself as a unique case worth investigating from the angle of end-users. We would like to change the perspective and look at the situation from the citizen's end. More specifically, we will approach the gap by focusing on what is actually driving them to use and accept eID. Although we are aware of the strategy and measures carried out by the Estonian government during its path of eID establishment, we want to find out what the citizens' perceptions and preferences are for the available eID means and what factors contribute to the existing level of eID public acceptance.

Identifying users' specific preferences, perceptions and attitudes is a potential source of feedback to service providers, policy makers and other stakeholders of the identity management domain [14].

Therefore, we investigate the following research questions:

1. Which eID authentication methods are preferred by the citizens?
2. What are the factors of eID public acceptance in Estonia?

We launch a survey targeting owners of Estonian eID and examine reasons, motivations, and features of eID usage and the potential appeal to end-users. As the Estonian eID consists of several solutions offered to citizens, we differentiate eID in the survey, so to obtain a more in-depth insight of attitudes and opinions. To interpret and frame the survey results, we use categories of eID public acceptance derived within previously conducted research. Additionally, we use statistical data on different eID means provided by the state eID issuer and trust service provider in order to analyze their usage more accurately. Within this research, we focus exclusively on the citizen as the end-user.

We begin our paper with defining our research methodology in Sect. 2. Next, we report on the findings in Sect. 3. We interpret and discuss the obtained results in the context of related work in Sect. 4. We finish with conclusion in Sect. 5.

2 Research Methodology

We used case study research [34] with a semi-structured qualitative survey as the data collection method [10,30]. We analyze the open-ended questions with thematic analysis. We argue that the chosen methodology serves best in achieving the research objectives, as we investigate the unique setting and state of affairs in the Estonia's identity management and enquire citizens' opinions.

We use pre-defined factors of eID acceptance derived from [32] to design the survey and interpret its result. Each factor is described in the context of our findings in the discussion section, i.e., Sect. 4. The list of factors is as follows (full definitions of the factors can be found in the original study [32]):

1. Complexity
2. Ease of use
3. Functionality
4. Awareness
5. Trust
6. Privacy
7. Security
8. Control and empowerment
9. Transparency.

We have ruled out the factors of "path dependency" and "cultural and historical factors" from the interpretation, as they are not relevant in the context of this research. We did not formulate the questions using or inquiring details from end-users related to the path chosen by the Estonian state when introducing eID defined as "path dependency", i.e. previous technical, organizational and regulatory settings [7]. Neither did we analyze the cultural and historical perspectives of the subject under research.

As there are several alternatives to access e-services available, we want to find out which functionalities and features appeal to users and what are the priorities when they choose a certain authentication method. Therefore, we designed a survey for the owners of Estonian eID, i.e. citizens, residents, individuals holding a digital citizenship (e-Residency), holders of digital identity cards. In total, we have collected n = 268 responses (Estonia has approx. 1,328,000 citizen, and approx. 97% of Estonian citizens have an eID [21], i.e., approx. N = 1.288.000, 95% confidence level with 6% margin). The survey was created in the online platform surveymonkey.com. We have used social media platforms and email channels to distribute the survey. As Estonia is a multi-lingual country the survey was distributed in three languages: Estonian, Russian, and English. The survey consisted of 12 questions.

The questions have covered eID relation to e-services, frequency of use, purpose, preferences for authentication options. When asking about e-services and their use we have distinguished between those provided by public and private sectors. We have also enquired what functionalities and features appeal to citizens the most. To get a general current picture of citizens' trust and attitudes, we have included the respective questions inquiring their opinions. We also included demographics-related questions on gender and age.

We also submitted requests for statistics from the Estonian eID issuer, Police and Border Guard Board (PBGB), and the trust services provider, SK ID Solutions AS (SK). They have provided data on the total number of online certificate status protocol (OCSP) requests, number of national eID part of the OCSP requests (all national documents including mobile-ID), mobile ID and Smart ID usage in numbers within the period of 01.01.2017–01.05.2019.

2.1 Limitations

One of the limitations of this research is the chosen method of sampling. Convenience sampling is not considered desirable and does not guarantee the representativeness of results for the entire population, i.e. the rest of Estonian citizens may have similar perceptions of eID [25].

Another aspect is that the provided statistical data is general and very limited in its range. We do not have access to specific numbers that reflect for example the usage of certain e-services depending on the authentication means. This would have been beneficial and helpful for a more precise analysis of user trends. However, acquiring such data would require contacting all e-services owners, both public and private.

To conclude, the identified features and factors are partly grouped according to categories derived from the previous research on eID public acceptance factors [32], which may not include all the variables that play a role in acceptance. In other words, this limitation emanates from the limitations of the previous research. Thus, we have also assumed the possibility to identify other novel and significant aspects worth outlining after analysis.

3 Results

We present the results of the survey by going through each of the questions and describing the breakdown of responses.

The first two questions aimed to obtain demographical data about respondents. 50.7% of respondents are male, 49.2% - female. The age groups are represented as follows: 32.4% (87 respondents) - 18–24 y. o., 32.8% (88 respondents) - 25–34 y. o., 22.7% (61 respondents) - 35–44 y. o., 7.4% (20 respondents) - 45–54 y. o., 1.8% (5 respondents) - 55–64 y. o., 2.2% (6 respondents) – older than 65 y. o.

Following the demographics, the respondents were asked what authentication methods they use in order to access e-services. Multiple choice was available. Figure 1 displays the answers. As it can be seen, ID card is used the most to access e-services. Smart ID holds the second position. Username/Password is the third choice with a rate of 47%. Mobile ID reached a similar percentage – 45.9%.

Further, the respondents were asked to specify how often they use e-services. 50% of respondents stated they are using e-services on a daily basis. Around 29%

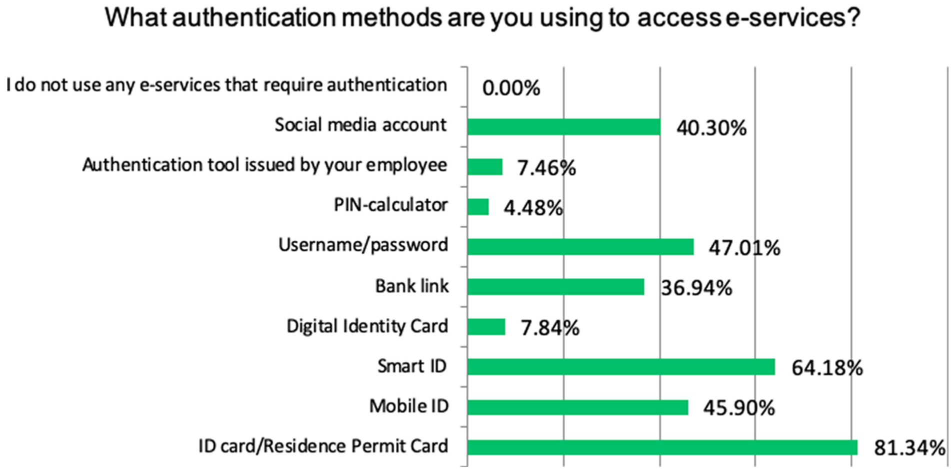


Fig. 1. eID authentication means

reported to use them at least several times a week, 8.9% - once a week, 9.7% - a few times a month, 1.8% - once a month, 0.7% - less than once a month. None of the respondents reported not using e-services at all.

Considering the wide range of available e-services, we decided to see also which are accessed using the available authentication means and which of those are the most prevailed depending on the service providers (public and private).

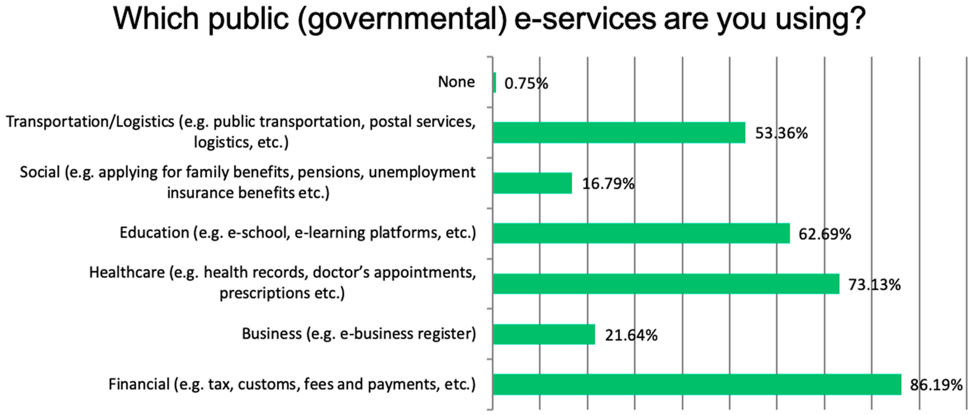


Fig. 2. Use of public e-services

As seen on Fig. 2, four types of services such as financial, healthcare, education, and transportation related e-services are clearly distinguished based on the responses. We have also listed e-services provided by private sector that require authentication and grouped them in categories such as transportation (e.g. taxi), entertainment, lifestyle, food delivery, telecommunication (e.g. mobile phone, internet), financial (e.g. banking). The results have reflected high numbers of private sector e-services used by respondents: transportation – 70,1%, entertainment – 60,4%, lifestyle – 78,7%, food delivery – 47,7%, telecommunications – 87,3%, financial – 90,6%.

When asked were there cases when users could not access an e-service by means of their preferred authentication method, 56,41% of respondents confirmed such cases occurred while the rest 43,5% replied negatively. Those who could not authenticated themselves were asked to clarify what was the service they had tried to access. 63% indicated it was a public service (e.g. many educational institutions do not support Smart ID; technical issues when using eID card or Digi-ID). The rest 36% of respondents reported private services not supporting their preferred options (e.g. certain banks not providing login with Smart ID).

The respondents were asked to explain their choice and/or preferences when using a particular authentication method among others. As the question was open-ended, we have analyzed the textual responses and created themes to sort them after skewing. We marked each response according to its theme and then summarized how many times each theme has occurred. Because many responses repeatedly included more than one theme, we present them separately as combined themes.

Table 1. Response summary to Q11.

Theme	# of times mentioned	% from total # of respondents
Convenience	41	18
Convenience + Security	17	6
Convenience + Speed	27	10
Convenience + Speed + Security	7	3
Ease of use	10	4
Security	8	6
Speed + Security	5	2
Speed	16	6
Usability	2	1
No additional device needed	5	2
Availability	5	2
Convenience in total	101	38
Security in total	38	14
Speed in total	65	25
Smart ID	45	17
ID card	20	8
Mobile ID	24	9
Username/Password	5	2
Social Media	2	1
PIN-Calculator	1	0

Among the responses, six types of authentication methods have been distinguished. Similarly, as in question about which methods are being used, respondents, again, featured Smart ID, Mobile ID, and ID card. The responses that contained themes on authentication methods were also occurring in combination with themes listed in the first part of the Table 1. For example, Smart ID + Convenience was mentioned three times; Smart + Mobile ID – four times.

Three themes such as Convenience, Speed, Security have been mentioned relatively frequently in combination with each other as well as standalone. Hence, we also summarized the number of times these themes were mentioned by the respondents in total. Convenience appeared as the most frequently named aspect and priority for respondents.

When asked what additional features users would prefer to utilize during authentication, we received the following results. The majority – 78.36% – of users indicated willingness to use fingerprints for authentication purposes. With respect to other biometrical data, 28.73% of users chose iris scan, 27.61% – facial image recognition as possible authentication options. Voice recognition appealed to 11.94% of respondents. A considerable number of users – 40.30% – would like to use NFC technology. It is worth noting that as of 2018 [30], a new generation of Estonian eID smart-cards are issued. The new ID document format supports NFC.

> Users have also written: *"I would only use fingerprint if it were an "additional" layer of security, not the only authentication needed to log in", "I have concerns about some of the abovementioned options. In particular concerns about security and reliability of those, especially given the modern technological advancements in AI (e.g. image rendering; voice reproduction). Hence, perhaps the only reasonable option is iris scan."*

Three respondents indicated their refusal to use the suggested options. Respondents have been also asked their opinion whether there are enough authentication methods available. The majority of almost 74% agreed there are enough, around 20% said there should be more, 3% there should be less, and around 3% replied *"I don't know."*

The next question on the possibility of having a universal solution has gained similar results where 64% of respondents would like to have several authentication options available, almost 28% found the idea to be appealing, and around 8% indicated they do not know. Some of the respondents have shared their comments with respect to the matter, pointing out the necessity of having more than one method available. One of the users found the idea of a universal solution to be utopian and the other expressed an opinion that considering the existing problems with eID, it is helpful that there are alternatives. Another point was made that having a single solution would have involved more risks and security concerns.

About 20% of respondents have indicated that they fully trust the service providers who handle their personal data. The same number of users noted they do have trust although not without some concerns. 36% feel skeptical about this matter but continue to use eID and e-services. About 3% express do not have trust and feel concerned about their data, and the same number of people do not understand how their data is handled and processed. Among the written responses, users note: *"Don't trust to e-elections"* and *"I trust public sector, and I'm skeptical of private sector."*

From the data provided by eID service providers, we have included for analysis the number of OCSP requests submitted via Mobile ID and Smart ID (See Fig. 3). OCSP is an Internet Protocol used for revocation of a digital certificate in the Public Key Infrastructure domain.

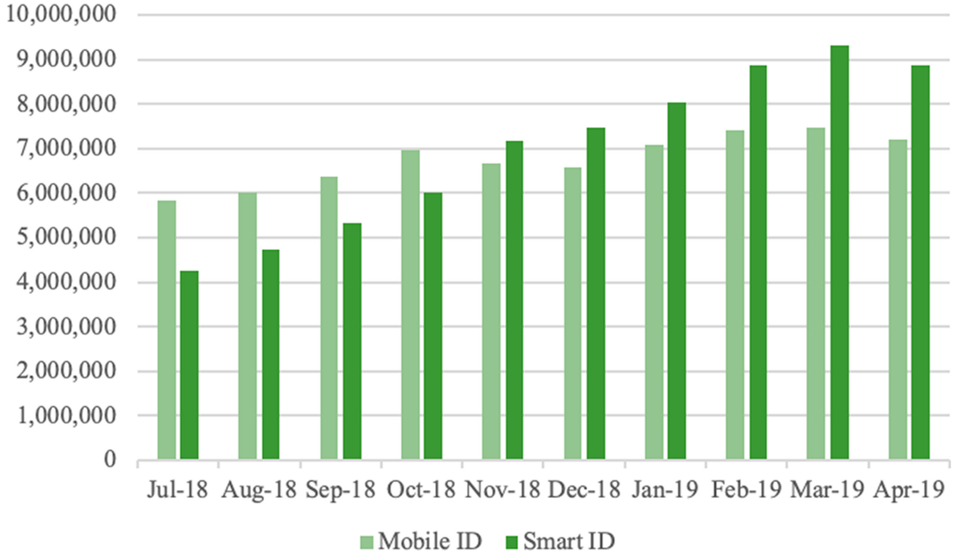


Fig. 3. Number of OCSP requests.

Mobile ID and Smart ID channels were the only differentiated arrays and thus significant for our study. The rest of data service providers decided to share with us were not included into analysis. The figures represented aggregated numbers that could not be applied within analysis which is why we could not relate to the rest of the results.

4 Discussion

4.1 eID Public Acceptance Factors

We will discuss our findings from the perspective of the eID public acceptance factors from Sect. 2 in combination with and against the background of related work. We interpret the Estonian eID according to the outcomes of empirical data analysis. We compare our insights with the ones discussed by other researchers.

Complexity. This factor explains to what extent users perceive the solution at use as a difficult-to-use system [27,32]. During the analysis of survey and written responses, no results were related to this factor.

Functionality. This factor refers to the perceived usefulness and benefit [11]. The results that reflect the types of e-services the respondents are accessing the most by various authentication methods, allow to conclude that the latter ones are seen useful and practical. 25% of respondents have mentioned speed as one of their priorities in choosing the right authentication method.

Awareness. Content analysis of written responses revealed that in general users are knowledgeable and tech-savvy. They demonstrate knowledge of potential risks when it comes to security and privacy, capabilities and limitations of the existing system, principles of its functioning, etc. For example, one user has mentioned the following when asked would a universal authentication method be better to use: *"The issue of technical capability. One central convenient working system would certainly be more convenient. However, given ID-card authentication issues, this problem would be greater if alternative authentication tools did not exist."* [5] argues that awareness is one of the bridges to understanding, trust and hence user acceptance. Additionally, [9] point to lack of awareness that leads to a perception of the technology being too complex. They further note building awareness as a way to enhance ease of use. The activities on the increasing awareness of Estonian population on the use of e-services have been evidently effective as the number of users has been growing [22].

Control and Empowerment. This factor refers to the citizen's ability to control his or her personal data and access to it. Moreover, it includes issues related to disclosure by consent, data integrity [15], access to services [1]. The analysis of collected data within this research did not extract results relevant to be interpreted with this factor.

Transparency. This factor refers to citizen's ability to understand the principles of his or her data is being processed by the service providers. It is also characterized as the visibility and accountability of brought to citizens through service delivery [1]. The question on the trust to service providers who handle personal data showed that only about 4% of respondents replied that they do not know or do not understand how their data is being handled. Though it seems to be the only aspect discovered that is relevant to this factor, it positively reflects on the given case.

Trust. It is assumed that public acceptance heavily relies on whether users trust the technology. Research results of a study aimed to identify public acceptance determinants of ten selected technologies detected trust to be a second most frequently occurring factor. In public sector, the concept of trust applies not only to the technology but to the service provider who must ensure and guarantee proper personal data processing. As within this research part of the respondents indicated to trust fully the service providers in handling their data (20%), demonstrated some concerns (19%), or felt skeptical about the matter

(36%), only around 4% of them showed themselves to be highly concerned, and the same number of people said they are not aware or do not understand how their data is handled. It can be said, that generally in case of Estonia the trust level is relatively high.

Privacy Concerns. This factor is tightly linked with trust. As privacy concerns comprise risks, the latter go hand-in-hand with trust. There is no consensus on how are they related. A study [29] revealed that trust is underpinned by the perceptions of risk. In the context of our research, as seen above, people do have a certain level of distrust towards service providers. A response was submitted where users have mentioned: *"Don't trust to e-elections"* and *"I trust public sector, and I'm skeptical of private sector."* Other types of technologies, for example, biometrics, used in identity management field, are associated with risks [18]. The respondents expressed they willingness to use biometrics but some shared the following opinions:

> *"I have concerns about some of the abovementioned options. In particular concerns about security and reliability of those, especially given the modern technological advancements in AI (image rendering; voice reproduction). Hence, perhaps the only reasonable option is iris scan."; "Prefer non-biometric options for privacy reasons but don't feel current tech allows for needed security. Smart ID is the best currently available in my opinion"; "I would only use fingerprint if it were an "additional" layer of security, not the only authentication needed to log in."*

The raised concerns do have a valid point. As [14] note, the concept of trust has been in focus of research in eCommerce primarily, where the trust of consumers is directed toward vendors not known previously, a situation of "initial trust". In this kind of a relationship, a predisposition to trust already exists. However, [29] argue, in public sector, the citizens, or "consumers" are too familiar with the service provider, i.e. state. In this sense, the technology itself is not an object of trust anymore but rather becomes an issue related to the service provider.

Security. This factor accounts for the ability of state, or service provider in general, to grant security of data, software, hardware, their reliability, trustworthiness, and safety. The importance of security is difficult to overestimate which is why it is not surprising that this issue has been raised by respondents when we asked about their priorities when choosing an authentication method. Security was mentioned in total 38 times.

Ease of Use. This factor has been defined as one of the major factors of public acceptance of technologies by many theories [11,33]. [11] defines ease of use as the "the degree to which a person believes that using a particular system would be free from effort". In this research, convenience (or ease of use) was the most frequently brought out theme by the respondents. As Table 1 demonstrates, it was mentioned as the priority more than 100 times. [9] mark convenience as one of the motivation factors of the acceptance of eID.

[6] indicates that "the ultimate convenience product or service would then be available continuously (time), everywhere (place), and would require almost no effort to acquire or use".

4.2 Authentication Methods

The results of the survey indicated several authentication methods users go for when it comes to e-services access. Almost each option has been featured by the respondents. A few points can be made in this regard. Firstly, the received numbers can be explained by range of available methods and a possibility to use them in parallel. Secondly, and this can be connected to the previous point, the responses showed that at least half of them are using e-services on a daily basis, while around one third uses them several times a week. Thirdly, given, that e-services are provided both by public and private sector and the authentication methods facilitated by these service providers can vary, we can say that one person uses at least two authentication methods. A governmental portal may offer to access its services by ID card and Mobile ID while, at the same time, the same user may visit, for instance, an insurance company's website authenticating himself with the same methods if available or with a username and password. The high percentage that reflects the use of ID card by respondents corresponds with the fact that 67% of Estonian population use ID card regularly as 99% of public services are available online [13,23]. A study on citizens' satisfaction of e-services conducted by the Ministry of Economic Affairs and Communication of Estonia indicated that "has increased on one hand due to an increased use of existing e-services as well as on the account of new e-services." [22] It was examined that within two years, the number of users of such e-services as healthcare, social affairs, transportation, financial affairs, increased significantly (20% growth in use on average).

It is difficult to distinguish a single leading authentication method. The respondents favor ID card, Mobile ID, Smart ID, and social media accounts. They also mostly agree that there is enough methods available and, moreover, a universal solution is not a good idea because users prefer to have alternatives. In 2017, Estonian e-identity management discovered a major security vulnerability known as ROCA (Return of Copper-Smith Attack) that affected more than 70% of e-ID cards [21]. Having at disposal alternative eID tokens was one of the key reasons why the stakeholders managed to go through the crisis smoothly without any radical actions that could compromise the state infrastructure's functioning. As the report on the lessons learned states, the incident has not affected the eID usage which has kept growing steadily since then [8]. The State Information System Authority as well as Police and Border Guard Board prioritized to retain people's trust during the crisis solving [21].

The collected data shows an increasing popularity of Smart ID. Ever since the establishment of the technology, the number of its users has been growing monthly until nowadays along with the number of transactions conducted by its means. It can be said with confidence, that Smart ID shortly after its launch has become one of the most preferred authentication means of Estonians. The written comments submitted within the survey confirm this.

In the initial stage of this research, when we were requesting statistical data on eID from the issuer and the trust service provides, unfortunately, it was not possible to obtain data which could reveal what is the most often-used authentication type. However, the growth of Smart ID usage can be seen from Fig. 3 where the number of OCSP requests via Smart ID can be compared with the ones sent via Mobile ID.

A study on the adoption of Smart ID in Estonia revealed that one of the effects on a rapid growth of usage was the knowledge about it, or in other words, awareness that spread through various service providers and peer networks [28]. In the case with service providers, Estonia again presents itself as an example of successful public-private partnership [20,21].

4.3 Future Work

There is no consensus on which authentication method is the best. Depending on the purpose, service being accessed, circumstances, devices available, options offered, the choice can be different. Looking at Estonia's setting, it may as well be the case, that the status quo in identity management is satisfactory. As a step further, it is planned to continue investigating Estonian case and collect more data, possibly, by arranging focus groups where users can discuss in detail each solution, and/or get additional input from service providers.

Bearing in mind the limitations of this study, we should look for more definitive answers to support the claims made. Moreover, as these claims are derived from self-reporting of respondents rather than measurement, the individuals could deliver inaccurate evaluations. The existing research on e-identity public acceptance relies on the concepts and theories such as Technology Acceptance Model, Diffusion of Innovations and their derivatives. In order to gain more confidence and validate the list of factors specifically created to characterize eID, further research is required. More specifically, it would be beneficial to design measurements for each factor, however, this in turn calls for a more in-depth both theoretical approach as well as empirical. This way, the accuracy of interpretation and assessment would increase significantly.

5 Conclusion

This research attempted to study citizens' attitudes and perceptions of Estonian eID using factors of eID public acceptance from our previous work. We addressed the stated research questions with the analysis of survey responses. Therefore, we identified the key priorities and preferences that drive users to make their choices and decisions when they use eID and which of the available options outstand.

The study asserts the uniqueness of Estonian case that is known for the advancements in the developments of digital society and e-government. The national e-ID scheme of Estonia is now announced as part of the state critical infrastructure [20,21]. This implies numerous dependencies of e-services functioning that citizens rely on and use on a daily basis. Among the top three factors that we used to interpret respondents' opinions, the most weight was given to ease of use or convenience. Though the concept of ease of use has been already proven multiple times to be a driver of technology adoption, we nevertheless insist on its importance in the context of Estonia which case is worth to learn lessons from. Functionality and Security that were oftentimes tied together with Ease of Use close up the three leading factors. Trust and Awareness were found to be contributing factors to the public acceptance. Respondents said they trust service providers who handle their personal data despite the fact that some concerns were expressed in this regard. This allowed to conclude that the general awareness and knowledge in the given field is relatively high. This is positively an advantage that the country possesses as mostly, findings from other research report this area as a weak spot.

Estonia offers several authentication options which seems to be if not the right thing to do, but, certainly, an effective strategy. Not only is this beneficial for the stable e-state functioning, but is also appealing to users that use them in parallel depending on the ever-changing circumstances.

Among the available authentication methods, certainly, a relatively new solution of Smart ID, launched in 2017, has become popular and continues to be used more and more. However, this trend does not reflect on the usage of ID card or Mobile ID that are keeping their positions. It can be said in other words, that, once again, no "one-size-fits-all" solution exists.

The case of Estonian e-identity management positively has lessons to offer, though the application of its "know-how" should be done selectively and on a context basis. Therefore, we lay ground and point to the need of further work to be conducted in the field of public acceptance of specific technologies such as eID also in other countries.

References

1. Aichholzer, G., Strauß, S.: The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. Identity Inf. Soc. **3**(1), 65–85 (2010). https://doi.org/10.1007/s12394-010-0048-9
2. Al-Hujran, O., Al-dalahmeh, M., Aloudat, A.: The role of national culture on citizen adoption of eGovernment services: an empirical study. Electron. J. e-Gov. **9**(2), 93–106 (2011)
3. Backhouse, J., Halperin, R.: A survey on EU citizens trust in ID systems and authorities. In: The European e-Identity Conference, pp. 1–31. FIDIS, Paris (2007). http://www.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizens_Trust.pdf
4. Backhouse, J., Halperin, R.: Security and privacy perceptions of e- ID: a grounded research. In: 16th European Conference on Information Systems, ECIS 2008, Galway, Ireland, 2008, pp. 1382–1393. Galway (2008)
5. Backhouse, J., Halperin, R.: Approaching interoperability for identity management systems. Future Identity Inf. Soc., 245–268 (2009). https://doi.org/10.1007/978-3-642-01820-6_6

6. Brown, L.G.: The strategic and tactical implications of convenience in consumer product marketing. J. Consum. Mark. **6**(3), 13 (1989). https://doi.org/10.1108/EUM0000000002550
7. Brugger, J., Fraefel, M., Riedl, R.: Raising acceptance of cross-border eID federation by value alignment. Electron. J. E-Gov. **12**(2), 178–188 (2014)
8. Buldas, A., et al.: ID-kaardi kaasuse õppetunnid. Technical report, Tallinn University of Technology, School of Information Technologies, Department of Software Science, Tallinn, Estonia (2018)
9. Chauhan, S., Kaushik, A.: Evaluating citizen acceptance of unique identification number in India: an empirical study. Electron. Gov. Int. J. **12**(3), 223–242 (2016). https://doi.org/10.1504/EG.2016.078416
10. Chigbu, U.E.: Visually hypothesising in scientific paper writing: confirming and refuting qualitative research hypotheses using diagrams. Publications **7**(22), 18 (2019). https://doi.org/10.3390/PUBLICATIONS7010022
11. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. **13**(3), 319–339 (1989). https://doi.org/10.2307/249008
12. De Cock, D., Simoens, K., Preneel, B.: Insights on identity documents based on the Belgian case study. Inf. Secur. Tech. Rep. **13**(2), 54–60 (2008). https://doi.org/10.1016/j.istr.2008.06.004
13. E-Estonia: e-Estonia — We have built a digital society and we can show you how. https://e-estonia.com/
14. Gupta, N., Fischer, A.R., Frewer, L.J.: Socio-psychological determinants of public acceptance of technologies: a review, October 2012. https://doi.org/10.1177/0963662510392485
15. Halperin, R., Backhouse, J.: A qualitative comparative analysis of citizens' perception of eIDs and interoperability. Technical report 507512, FIDIS (2009)
16. ID.ee: ID.ee. https://www.id.ee/?lang=en&id=
17. Kalja, A.: The first ten years of X-Road. Est. Inf. Soc. Yearb. **2011**(2012), 78–80 (2012)
18. Kalvet, T., Tiits, M., Laas-Mikko, K.: Public acceptance of advanced identity documents. In: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance - ICEGOV 2018, pp. 429–432. ACM Press, New York (2018). https://doi.org/10.1145/3209415.3209456
19. Khatchatourov, A., Laurent, M., Levallois-Barth, C.: Privacy in digital identity systems: models, assessment, and user adoption. In: Tambouris, E., et al. (eds.) EGOV 2015. LNCS, vol. 9248, pp. 273–290. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22479-4_21
20. Lips, S., Aas, K., Pappel, I., Draheim, D.: Designing an effective long-term identity management strategy for a mature e-State. In: Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) EGOVIS 2019. LNCS, vol. 11709, pp. 221–234. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27523-5_16
21. Lips, S., Pappel, I., Tsap, V., Draheim, D.: Key factors in coping with large-scale security vulnerabilities in the eID field. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2018. LNCS, vol. 11032, pp. 60–70. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98349-3_5
22. Ministry of Economic Affairs and Communication: Estonian populations' satisfaction with public e-services 2014. Technical report, Ministry of Economic Affairs and Communications (2014)

23. Ministry of Foreign Affairs: E-services for citizens e-Elections e-Tax Board. Technical report, Ministry of Foreign Affairs, Republic of Estonia, Tallinn, Estonia (2014). vm.ee
24. Pappel, I., Pappel, I., Tepandi, J., Draheim, D.: Systematic digital signing in Estonian e-Government processes. In: Hameurlain, A., Küng, J., Wagner, R., Dang, T.K., Thoai, N. (eds.) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI. LNCS, vol. 10720, pp. 31–51. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-56266-6_2
25. Patton, M.Q.: Designing qualitative studies. In: Qualitative Research and Evaluation Methods, 3 edn. Chap. 5, pp. 207–257. SAGE Publications, Thousand Oaks (2002)
26. Priesnitz Filho, W., Ribeiro, C., Zefferer, T.: Privacy-preserving attribute aggregation in eID federations. Future Gener. Comput. Syst. **92**, 1–16 (2019). https://doi.org/10.1016/j.future.2018.09.025
27. Robles, G., Gamalielsson, J., Lundell, B.: Setting up government 3.0 solutions based on open source software: the case of X-Road. In: Lindgren, I., et al. (eds.) EGOV 2019. LNCS, vol. 11685, pp. 69–81. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27325-5_6
28. Sai, A.A.: An exploratory study of innovation adoption in Estonia. Open J. Bus. Manag. **06**(04), 857–889 (2018). https://doi.org/10.4236/ojbm.2018.64064
29. Sjöberg, L.: Attitudes toward technology and risk: going beyond what is. Policy Sci. **35**, 379–400 (2002)
30. van Thiel, S.: A survey. In: Research Methods in Public Administration and Public Management: An Introduction, 1st edn., vol. 9780203078, Chap. 7, pp. 1–196. Taylor and Francis, London (2014). https://doi.org/10.4324/9780203078525
31. Tsap, V., Pappel, I., Draheim, D.: Key success factors in introducing national e-identification systems. In: Dang, T.K., Wagner, R., Küng, J., Thoai, N., Takizawa, M., Neuhold, E.J. (eds.) FDSE 2017. LNCS, vol. 10646, pp. 455–471. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70004-5_33
32. Tsap, V., Pappel, I., Draheim, D.: Factors affecting e-ID public acceptance: a literature review. In: Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) EGOVIS 2019. LNCS, vol. 11709, pp. 176–188. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27523-5_13
33. Venkatesh, M., Davis, D.: User acceptance of information technology: toward a unified view. MIS Q. **27**(3), 425 (2003). https://doi.org/10.2307/30036540
34. Yin, R.K.: Case Study Research and Applications, 6 edn. SAGE Publications Inc., Los Angeles (2019). https://doi.org/10.1017/CBO9781107415324.004

Curriculum Vitae

Personal data

Name	Valentyna Tsap
Date and place of birth	13 August 1994, Ternopil, Ukraine
Nationality	Ukrainian

Contact Information

Address	Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Estonia
Phone	+372 59191138
E-mail	valentyna.tsap@cyber.ee

Education

2017–...	Tallinn University of Technology, School of Information Technology, PhD
2015–2017	Tallinn University of Technology, School of Information Technology, e-Governance technologies and services, MSc
2011–2015	Ternopil National Economic University, Educational and Scientific Institute of International Economic Relations, International Information, BSc

Language Competence

English	fluent
Ukrainian	native
Russian	fluent
Estonian	intermediate

Professional Employment

2021– ...	Cybernetica AS, Junior Analyst
2017–2021	Tallinn University of Technology, Early Stage Researcher

Defended Theses

- 2015, "Ukrainian eID: Its Aspects and Citizens' Awareness towards It", MSc, supervisor Assoc. Prof. Ingrid Pappel, Tallinn University of Technology, Department of Software Science
- 2015, "International Scientific and Information Exchange", BSc supervisor Prof. Oksana Lyashenko, Ternopil National Economic University, Educational and Scientific Institute of International Economic Relations

Fields of Research[2]

4.6. Computer Science
4.7. Information and Communications Technologies

[2] Estonian Research Information System (ETIS) fields of research

Scientific work

1. I. Pappel, V. Tsap, and D. Draheim. The e-LocGov model for introducing e-governance into local governments: an Estonian case study. *IEEE Transactions on Emerging Topics in Computing*, 9(2):597–611, 2021

2. A. R. Mærøe, A. Norta, V. Tsap, and I. Pappel. Increasing citizen participation in e-participatory budgeting processes. *Journal of Information Technology & Politics*, 18(2):125–147, 2021

3. A. Valtna-Dvořák, S. Lips, V. Tsap, R. Ottis, J. Priisalu, and D. Draheim. Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2021 – the 10th International Conference Electronic Government and the Information Systems Perspective*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer

4. Y. Petriv, R. Erlenheim, V. Tsap, I. Pappel, and D. Draheim. Designing effective chatbot solutions for the public sector: a case study from Ukraine. In A. Chugunov, I. Khodachek, Y. Misnikov, and D. Trutnev, editors, *Proceedings of EGOSE'2019 – the 6xt International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, volume 1135 of *Communications in Computer and Information Science*, pages 320–335, Cham, 2020. Springer

5. V. Tsap, S. Lips, and D. Draheim. eID public acceptance in Estonia: towards understanding the citizen. In S.-J. Eom and J. Lee, editors, *Proceedings of dg.o'20 – the 21st Annual International Conference on Digital Government Research: Intelligent Government in the Intelligent Information Society*, pages 340–341. Association for Computing Machinery, 2020

6. V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In A. Kö, E. Francesconi, G. Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2020 – the 9th International Conference on Electronic Government and the Information Systems Perspective*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer

7. I. Pappel, V. Tsap, I. Pappel, and D. Draheim. Exploring e-services development in local government authorities by means of electronic document management systems. In A. Chugunov, Y. Misnikov, E. Roshchin, and D. Trutnev, editors, *Proceedings of EGOSE'2018 – the 5th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, volume 947 of *Communications in Computer and Information Science*, pages 223–234, Cham, 2019. Springer

8. K. Kreos, E. Täks, V. Tsap, I. Pappel, and D. Draheim. On facilitating cross-border e-commerce through an automated VAT declaration system. In L. Terán, A. Meier, and J. Pincay, editors, *Proceedings of ICEDEG'2019 – the 6xt International Conference on eDemocracy & eGovernment*, pages 56–63. IEEE, 2019

9. O. Popelyshyn, V. Tsap, I. Pappel, and D. Draheim. On leveraging the potential of open data to enhance transparency and accountability – a case study from Ukraine. In L. Terán, A. Meier, and J. Pincay, editors, *Proceedings of ICEDEG'2019 – the 6xt International Conference on eDemocracy & eGovernment*, pages 25–30. IEEE, 2019

10. M. Ruus, I. Pappel, V. Tsap, and D. Draheim. Enhancing public e-service delivery: Recognizing and meeting user needs of youngsters in Estonia. In D. A. Alexandrov, A. V. Boukhanovsky, A. V. Chugunov, Y. Kabanov, O. Koltsova, and I. Musabirov, editors, *Proceedings of DTGS'2019 – the 4th International Conference on Digital Transformation & Global Society*, volume 1038 of *Communications in Computer and Information Science*, pages 29–40. Cham, 2019

11. V. Tsap, I. Pappel, and D. Draheim. Factors affecting e-ID public acceptance: A literature review. In A. Kő, E. Francesconi, G. Anderst-Kotsis, A M. Tjoa, and I. Khalil, editors, *Proceedings of EGOVIS'2019 – the 8th International Conference on Electronic Government and the Information Systems Perspective*, pages 176–188, Cham, 2019. Springer

12. M. Tsulukidze, K. Nyman-Metcalf, V. Tsap, I. Pappel, and D. Draheim. Aspects of personal data protection from state and citizen perspectives – case of Georgia. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, and M. Mäntymäki, editors, *Proceedings of I3E'2019 – the 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society: Digital Transformation for a Sustainable Society in the 21st Century*, volume 11701 of *Lecture Notes in Computer Science*, pages 476–488, Cham, 2019. Springer

13. S. Lips, V. Tsap, I. Pappel, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In A. Kõ and E. Francesconi, editors, *Proceedings of EGOVIS'2018 - the 7th International Conference on Electronic Government and the Information Systems Perspective*, volume 11032 of *Lecture Notes in Computer Science*, pages 60–70, Cham, 2018. Springer

14. M. Järvsoo, A. Norta, V. Tsap, I. Pappel, and D. Draheim. Implementation of information security in the EU information systems: an Estonian case study. In S. A. Al-Sharhan, A. C. Simintiras, Y. K. Dwivedi, M. Janssen, M. Mäntymäki, L. Tahat, I. Moughrabi, T. M. Ali, and N. P. Rana, editors, *Proceedings of I3E'2018 – the 17th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society: Challenges and Opportunities in the Digital Era*, volume 11195 of *Lecture Notes in Computer Science*, pages 150–163, Cham, 2018. Springer

15. V. Tsap and I. Pappel. Roundtable: Maturity of national eIDs. In *Abstracts of Papers Presented at the 18th European Conference on Digital Government ECDG 2018: University of Santiago de Compostela Spain, 25-26 October 2018*, page 46. Academic Conferences and Publishing International Limited, 2018

16. V. Tsap. e-Identity and eIDAS: Interpretation of concepts by different countries. In A.-M. Osula and O. Maennel, editors, *Proceedings of ICR'2018 – the 4th Interdisciplinary Cyber Research Workshop 2018*, pages 9–10. Tallinn University of Technology, Department of Software Science, 2018. [last accessed 5 Nov 2021] https://haldus.taltech.ee/sites/default/files/2021-04/ICR2018_proceedings.pdf

17. V. Tsap, I. Pappel, and D. Draheim. Key success factors in introducing national e-identification systems. In T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, editors, *Proceedings of FDSE'2017 – 4th International Conference on the Future Data and Security Engineering*, volume 10646 of *Lecture Notes in Computer Science*, pages 455–471, Cham, 2017. Springer

Elulookirjeldus

Isikuandmed

Nimi	Valentyna Tsap
Sünniaeg ja -koht	13.08.1994, Ternopil, Ukraina
Kodakondsus	Ukraina

Kontaktandmed

Aadress	Cybernetica AS, Mäealuse 2/1, 12618 Tallinn, Estonia
Telefon	+ 372 59191138
E-post	valentyna.tsap@cyber.ee

Haridus

2017–. . .	Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, doktoriõpe
2015–2017	Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, e-Riigi tehnoloogiad ja teenused, MSc
2011–2015	Ternopili Rahvamajanduseülikool, Rahvusvaheliste Majandussuhete Haridus- ja Teadusinstituut, Rahvusvaheline Informatsioon, BSc

Keelteoskus

inglise keel	kõrgtase
ukraina keel	emakeel
vene keel	kõrgtase
eesti keel	kesktase

Teenistuskäik

2021– . . .	Cybernetica AS, nooremanalüütik
2017–2021	Tallinna Tehnikaülikool, nooremteadur

Kaitstud lõputööd

- 2017, "Ukraina eID: Selle Rakendamise Aspektid ja Kodanike Teadlikkus", MSc, juhendaja dotsent. Ingrid Pappel, Tallinna Tehnikaülikool, Tarkvarateaduste instituut
- 2015, "Rahvusvaheline teadus- ja teabevahetus", BSc, juhendaja Prof. Oksana Lyashenko, Ternopili Rahvamajanduseülikool, Rahvusvaheliste Majandussuhete Haridus- ja Teadusinstituut

Teadustöö põhisuunad[3]

4.6. Arvutiteadused
4.7. Info- ja kommunikatsioonitehnoloogia

[3] Eesti Teadusinfosüsteemi (ETIS) teadusvaldkondade ja -erialade klassifikaator

ISSN 2585-6901 (PDF)
ISBN 978-9949-83-801-1 (PDF)