TAL TECH

DOCTORAL THESIS

A Multifaceted Assessment Framework for Electronic Identity Schemes

Silvia Lips

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2023

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
34/2023

A Multifaceted Assessment Framework for Electronic Identity Schemes

SILVIA LIPS

TAL TECH PRESS

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 03 July 2023

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

Co-supervisor: Prof. Dr. Dr. Robert Krimmer,
Johan Skytte Institute of Political Studies,
University of Tartu,
Tartu, 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.ir. M.F.W.H.A. (Marijn) Janssen,
Faculty of Technology, Policy and Management,
Delft University of Technology,
Delft, the Netherlands

Prof. Dr. Gabriele Kotsis,
Department of Telecooperation,
Johannes Kepler University Linz,
Linz, Austria

Defence of the thesis: 04 September 2023, 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.

Silvia Lips _____
signature

ISSN 2585-6898 (publication)
ISBN 978-9916-80-020-1 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-021-8 (PDF)
Printed by Koopia Niini & Rauam

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
34/2023

Elektrooniliste autentimisskeemide mitmetahuline hindamise raamistik

SILVIA LIPS

TAL TECH
KIRJASTUS

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 S. Lips, V. Tsap, N. Bharosa, R. Krimmer, D. Draheim, and T. Tammet. Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia. In *Information Systems Frontiers*, 2023

II S. Lips, N. Vinogradova, R. Krimmer, and D. Draheim. Re-shaping the EU digital identity framework. In *the 23rd Annual International Conference on Digital Government Research*, dg.o 2022, page 13–21, New York, NY, USA, 2022. Association for Computing Machinery

III S. Lips, R. K. Ahmed, K. Zulfigarzada, R. Krimmer, and D. Draheim. Digital sovereignty and participation in an autocratic state: Designing an e-petition system for developing countries. In *the 22nd Annual International Conference on Digital Government Research*, dg.o 21, page 123–131, New York, NY, USA, 2021. Association for Computing Machinery

IV S. Lips, N. Bharosa, and D. Draheim. eIDAS implementation challenges: the case of Estonia and the Netherlands. In *the 7th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2020, pages 75–89, 2020

V S. Lips, K. Aas, I. Pappel, and D. Draheim. Designing an effective long-term identity management strategy for a mature e-state. In *the 8th Electronic Government and the Information Systems Perspective*, EGOVIS 2019, pages 221–234, Cham, 2019. Springer

VI S. Lips, I. Pappel, V. Tsap, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In *the 7th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2018, pages 60–70, 2018

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

VIII V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In *the 9th International Conference on Electronic Government and the Information Systems Perspective, EGOVIS 2020*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer

IX R. K. Ahmed, K. H. Muhammed, A. O. Qadir, S. I. Arif, S. Lips, K. Nyman-Metcalf, I. Pappel, and D. Draheim. A legal framework for digital transformation: A proposal based on a comparative case study. In *the 10th International Conference on Electronic Govern-ment and the Information Systems Perspective*, EGOVIS 2021, pages 115–128, Cham, 2021. Springer

X M. S. H. A. Sallam, S. Lips, and D. Draheim. Success and success factors of the Estonian e-residency from the state and entrepreneur perspective. In *the 8th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2021, pages 291–304, Cham, 2022. Springer

XI 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 *the 10th International Conference Electronic Government and the Information Systems Perspective, EGOVIS 2021*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer

XII R. Saputro, I. Pappel, H. Vainsalu, S. Lips, and D. Draheim. Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study. In *the 7th International Conference on eDemocracy & eGovernment, ICEDEG 2020*, pages 216–222, 2020

XIII 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, *Electronic Participation*, pages 41–53, Cham, 2020. Springer

Author's Contributions to the Publications

I In I, I was the first author of the publication. I conducted the expert interviews, analysed them, proposed the research design and wrote and edited the manuscript under the guidance of my supervisor. The publication was submitted to the journal Information Systems Frontiers in 2022.

II In II, I was the first author of the publication. The publication bases partly on a master´s thesis that I supervised. I analysed the eIDAS Regulation proposal and compared the results with the results of the master´s thesis. I designed the research structure and wrote the manuscript of the publication. I presented the publication online at the International Conference on Digital Government Research in 2022.

III In III, I was the first author of the publication. The publication bases on a master´s thesis that I supervised. I proposed the research design and wrote the manuscript of the publication. I presented the publication online at the International Conference on Digital Government Research in 2021.

IV In IV, I was the first author of the publication. I was responsible for the overall coordination of the expert meeting between the Estonia and the Netherlands. I designed the workshop format, facilitated the workshops, participated actively in the discussions and documented the workshops results. Finally, I prepared the publication manuscript. I presented the publication online at the International Conference on Electronic Governance and Open Society: Challenges in Eurasia in 2020.

V In V, I was the first author of the publication. I was coordinating the identity management and identity documents strategy building process and wrote my master´s thesis about this topic. The publication relies on the collected date and main findings of the thesis. I conducted the expert interviews, analysed the results, prepared the figures, tables and wrote the manuscript under the guidance of my supervisor. The author presented the publication at the International Conference on Electronic Government and the Information Systems Perspective in Linz, Austria, 2019.

VI In VI, I was the first author of the publication. I proposed the overall research design and contributed to the manuscript writing by describing the eID ecosystem, the security vulnerability and the key factors that helped to overcome it. By the time of writing the manuscript, I was working at the Estonian Police and Border Guard Board (PBGB) and I was responsible for solving the incident analyzed in the publication. Therefore, I also participated in the publication writing process as an PBGB expert.

VII In VII, I was the second author of the publication. I helped the main author with the research design. I also helped to design the survey questions and participated actively in the publication related discussions.

VIII In VIII, I was the second author of the publication. I helped to design the research structure and participated in the survey design. I reviewed the publication manuscript before the submission.

IX In IX, I conducted the Estonian e-government legislation analysis in the e-court context. I helped to draft the publication manuscript and participated in the publication related discussions.

X In X, I was the second author of the publication. The publication bases on a master´s thesis that I supervised. I proposed the research design, helped to design the interview questions and to find the interviewees. I drafted the manuscript and edited it according to the reviewers feedback. I presented the publication online at the International Conference on Electronic Governance and Open Society: Challenges in Eurasia in 2021.

XI In XI, I was the second author of the publication. I drafted the manuscript and coordinated the publication writing process. I provided my expert input to the publication by being one of the interviewees as I was working at the PBGB when the security vulnerability appeared and I was directly involved in solving it.

XII In XII, I drafted the manuscript, edited it according to the reviewers feedback and prepared the camera-ready version of the publication. I also participated in the publication related discussions.

XIII In XIII, I was the second author of the publication. I was responsible for the overall coordination of the expert meeting between the Estonia and the Netherlands and participated actively in the e-government related discussions.

Abbreviations

ANSSI	French National Cybersecurity Agency/Agence nationale de la sécurité des systèmes d'information
ARF	Architecture and Reference Framework
A-SIT	Secure Information Technology Center – Austria
BOSA	Belgian Federal Public Service Policy and Support
BSI	Federal Office for Information Security/Bundesamt für Sicherheit in der Informationstechnik
CAS	Complex Adaptive Systems
CBA	Cost-Benefit analysis
CEF	Connecting Europe Facility
CEN	European Committee for Standardisation
CN	Cooperation Network
COTW	Coalition of the Willing
CSA	European Union Cybersecurity Act
CTA	Constructive Technology Assessment
DS	Design Science
EC	European Commission
ECCG	European Cybersecurity Certification Group
EEA	European Economic Area
EGDI	E-Government Development Index
eID	Electronic Identity
eIDAF	Assessment Framework of eID Schemes
eIDAS	Regulation 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
ENISA	European Union Agency for Cybersecurity
EPTA	European Parliamentary Technology Assessment
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	European Digital Identity
EWC	EUDI Wallet Consortium
GDPR	General Data Protection Regulation
IIA	Inception Impact Assessment
IdP	Identity Provider
ISA	Information System Authority
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
LCA	Life cycle analysis
LoA	Level of Assurance
LSP	Large Scale Pilot
MEG	Mobile eGovernment key
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NOBID	The Nordic-Baltic eID Project
ODI	Organisational Digital Identity
OOP	Once-Only Principle
OPT	One-Time Password
PBGB	Police and Border Guard Board

PKI	Public Key Infrastructure
ROCA	Return of Coppersmith's attack
SAML	Security Assertion Markup Language
SDGR	Single Digital Gateway Regulation
SSI	Self-Sovereign Identity
SRQ	Sub-research question
TA	Technology Assessment
UN	United Nations
WG	Working Group

Terms

Authoritative source	According to the Implementing Regulation (EU) 2015/1502, the authoritative source can be any source independent of its format that can be relied upon to provide accurate data, information and/or evidence in the identity proofing process.
eID means	According to the eIDAS regulation means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
eID scheme	According to the eIDAS regulation means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons.
Level of assurance (LoA)	According to ISO/IEC 29115, a LoA describes “the degree of confidence in the processes leading up to and including the authentication process itself, thus providing assurance that the entity claiming a particular identity (i.e., the entity) is in fact the entity to which that identity was assigned”. According to the eIDAS regulation, an eID scheme can be notified on assurance levels "low", "substantial" and/or "high" [42].
Peer review	According to article 7 of the Implementing Decision (EU) 2015/296, peer review is a mechanism for cooperation between member states designed to ensure interoperability and security of the notified electronic identification schemes.

1 Introduction

Electronic identification of users is an essential component of the digital society enabling safe and high-quality e-service provision. Therefore, it is vital that service providers can be sure that they provide services to the correct persons. In the public sector, the authentication of users is particularly relevant as accurate identification is directly related to trust in the government and its services. However, from the user´s perspective, the authentication procedure is often seen as a formality they would rather skip. Therefore, public and private sector service providers are motivated to find a balance between secure and conveniently usable authentication solutions. Moreover, the need for cross-border service provision has increased over the years, bringing interoperability aspects of authentication into the discussions.

This research focuses on European countries' electronic identity (eID) schemes and analyses the current eID cross-border recognition process. This dissertation aims to facilitate the interoperable use of eIDs in the European internal market by proposing a multifaceted assessment framework for electronic identity schemes, moreover, with the perspective to apply the framework in cross-border use cases with third countries.

According to the latest United Nations (UN) e-Government survey, all European Union (EU) countries have a very high e-Government Development Index (EGDI) [174]. Furthermore, the survey shows that eight European countries are among the top 15 leading countries in e-government development in the world [174]. However, being all highly ranked, each country is unique and has built its technical ecosystem. Therefore, it is impossible to accept the systems automatically for cross-border use.

The mutual recognition of member states eID schemes is the basis of the current European eID interoperability framework. To ensure a high-security level and comparability of the eID schemes of different countries, the European Commission has established a Cooperation Network (CN) consisting of member state eID experts who assess the eID schemes based on peer review. The author of this dissertation has been a representative of Estonia in the CN since 2021 and participated in the eID schemes peer reviews of Sweden, Norway, the Czech Republic, the Netherlands, Austria, Denmark, Liechtenstein, Poland, Bulgaria and Slovenia.

However, the peer-review process is time-consuming and bureaucratic. With the pre-notification, administrative procedures, and implementation, the peer-review process may take one to 1.5 years. Considering the constantly changing technological environment and cybersecurity situation, ensuring that the peer-review process is effective and enables the notification of the changes made in the national eID schemes operatively is essential.

The need for transparent, secure, and fluently functioning cross-border authentication solutions and analysis of the existing time-consuming peer review process leads to the main research question of this dissertation:

- How to design a framework for assessing electronic identity schemes?

Answering this question presumes an in-depth understanding of the national eID practices, an analysis of the eIDAS regulation and its implementation in EU countries, as well as an analysis of the existing eID peer review routines. Therefore, the author constructed three auxiliary research questions for the main research question.

- What are the different eID practices at the level of the member states in terms of eIDAS implementation? (National eID practice analysis) (SRQ1)

- Which challenges have been encountered by the member states during the eIDAS

implementation, stemming from EU eIDAS practice? (EU eIDAS practice analysis) (SRQ2)

- How do the member states recognise eID schemes of other countries to enable the cross-border e-service provision? (SRQ3)

Before it is possible to design a multifaceted assessment framework for eID schemes, it is essential to understand national eID practices and how eID ecosystems work. Therefore, the author analyses Estonian eID technical solutions, Estonian eID stakeholders, and the Estonian eID strategy. The interoperability perspective requires a broader analysis at the European level. For that purpose, the author focused on the eIDAS implementation practices. The aim was to identify member states' challenges during the eIDAS implementation. After understanding the national and EU perspective, it was possible to focus on the processes enabling the interoperable usage of the eID schemes.

To propose the multifaceted assessment framework for eID schemes (eIDAF), the author follows a design science (DS) research methodology. Three theoretical concepts support the research activities,i.e., identity theory [25], institutional design by Koppenjan and Groenewegen [80], and technology assessment (TA) [54, 53]. Identity theory helps to understand different aspects of identity and how these identities are connected [25]. Institutional design by Koppenjan and Groenewegen provides a framework for describing complex socio-technological systems and is suitable for multi-layer ecosystems like eID [80]. Finally, the technology assessment approach addresses the social and technological challenges and offers different methods that the author analyses while proposing the assessment framework for eID schemes [54, 53]. During the research, the author used qualitative and quantitative data collection methods. Finally, the research results are validated using expert interviews and three scenarios (Denmark, the Czech Republic, and the Netherlands).

This dissertation consists of thirteen chapters. In the introduction in Chapter 1, the author introduces the research question and the research aim. In Chapter 2, the author presents the overall research design and methodology. Chapter 3 overviews the eID and eIDAS related literature. Chapters 4 and 5 form the dissertation's theoretical and practical background. Chapter 4 describes three theoretical concepts (identity theory, institutional design by Koppenjan and Groenewegen, and technology assessment) that the author uses as a theoretical basis for the dissertation. Chapter 5 provides an overview of the eIDAS regulation and its stakeholders and describes the eID schemes notification process together with the list of already notified eID schemes. Moreover, the author gives a short overview of the practical implementation of the eIDAS regulation. Chapter 6 focuses on analyzing of the existing eID peer review routines in the EU, followed by the expert interview results presentation in Chapter 7. Chapter 8 introduces a multifaceted assessment framework for eID schemes designed by the author. Chapter 9 presents the evaluation interview results and recommendations made by the experts. Chapter 10 describes peer review scenarios of three countries (Denmark, the Czech Republic, and the Netherlands) as a part of the evaluation. The author provides an overview of the research limitations in Chapter 11 and discusses the future research perspective in Chapter 12. The author concludes the dissertation in Chapter 13.

2 Research Design and Methodology

This chapter provides an overview of the research design of the dissertation and describes in detail the used research methodology and data collection methods. Firstly, the author introduces the overall research design, then gives a detailed overview of how the research methodology was applied and how the data was collected. Finally, the author describes the research results validation procedure.

2.1 Research Design

This research is designed inductively using a bottom-up approach. To develop an assessment framework for the cross-border use of eID schemes, understanding the concept of electronic identity and how it works nationally is essential. Then it is possible to move to the more complex levels. Therefore, the author started the research activities from the national eID practice analysis and continued the work at the EU level.

The author follows the logic of a complex adaptive systems (CAS) model to frame the research design [106] and integrates it into the eID context. CAS model fits perfectly for the eID systems as it reflects the connection between the individual and collective level of using information and communication technology-based solutions [106]. It also represents the close interrelation between the user, technology, and e-services. Moreover, the author added the normative environment dimension to the model as it plays a significant role in the eID field on both levels.

Fig 1 presents the multifaceted approach of this research. First, the author started the study from the individual level and analysed national eID practices from different perspectives, answering the first auxiliary question, "What are the different eID practices at the level of the member states in terms of eIDAS implementation?" (SRQ1).

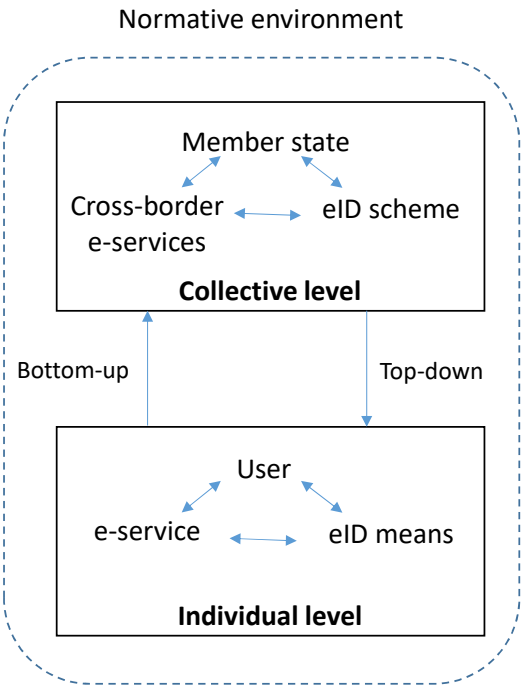

Figure 1: Research design. Model design by author based on a CAS model [106].

Table 1 provides an overview of the publications that answer SRQ1. Using Estonia as a case study, the author covers three different layers (user, eID means, and e-service) at the individual level. More specifically, the author addressed the following main topics in the publications:

- eID stakeholders analysis (publications I, V, VI, XI, X);
- eID token analysis (publications, V, VI, X);
- role of the eID in the e-service provision (publications I, V, VI, XI, X);
- security incident management in the eID context (publications VI, XI);
- eID as a state critical infrastructure component (publications I, VI);
- national eID strategy building (publication V);
- Estonian e-residency project analysis (publication X);
- eID public acceptance in Estonia and user preferences (publications VII, VIII);
- eID infrastructure components analysis (publications I, VI, XII);
- eID legal framework analysis (publications V, IX).

Table 1: Correlation of the research publications to the research questions

How to design a framework for assessing electronic identity schemes?													
SRQ No	**I**	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**IX**	**X**	**XI**	**XII**	**XIII**
SRQ 1	X				X	X	X	X	X	X	X	X	
SRQ 2		X		X									X
SRQ 3		X	X	X	X								X

Table 1 provides an overview of the publications that answer SRQ2. The author covers the member state view, eID scheme notification, and cross-border use of eIDs under the eIDAS regulation. The author covered the following main aspects:

- analysis of the eIDAS Regulation development (publications II, IV, XIII);
- eIDAS Regulation implementation challenges analysis according to the practice of Estonia and the Netherlands (publications II, IV);
- analysis of the stakeholder´s expectations towards the eIDAS Regulation (publications II, IV).

Those publications focused on the national eID practice in-depth analysis, providing valuable input to further research from the user, technology, and organisational perspective. Moreover, the author analysed the eID from the critical infrastructure point of view.

The research activities continued on the collective level. The author analysed eID practices and eIDAS Regulation and its implementation challenges in other EU countries. Moreover, the author researched the revised version of the eIDAS Regulation (eIDAS v2). As a result, the second auxiliary question, "Which challenges have been encountered by the member states during the eIDAS implementation, stemming from EU eIDAS practice?" (SRQ2), was answered.

Based on the input from the individual and collective level, together with the analysis provided in this dissertation, it was possible to answer the third auxiliary question, "How do the member states recognise eID schemes of other countries to enable the cross-border e-service provision?" (SRQ3). Responding to this question presumed well-organized analysis through different organisational and technical layers of the eID ecosystem. Therefore, the author decided to rely on the theoretical concept of the institutional design for complex technological systems proposed by Koppenjan and Groenewegen [80].

Table 1 provides an overview of the publications that help to answer SRQ3. In addition to the member state practice analysis, the author had to research the legislative environment separately to answer the SRQ3. The author analysed member state eID practices, normative environment, and internal processes, focusing on the following aspects:

- organisational role division and responsibilities in the member states in the eID schemes recognition process (publications IV, V, XIII and Section 5);
- normative environment analysis (publications III, IV, V, IX and Section 5);
- mutual recognition process analysis (publication IV and Section 6);
- mutual recognition practice analysis based on the expert feedback (Section 7).

This dissertation combines the paradigms of pragmatism and interpretivism [51, 100]. Pragmatism formulated by philosophers Peirce, James, Dewey, and Mead is often linked with constructive knowledge, action, and intervention and is suitable for qualitative research in information systems [51]. The application of pragmatism can be seen in the last part of this research when the author focuses on how experts peer review the eID schemes in practice [50]. Moreover, pragmatism is a suitable approach in the case of design science research [51], which is used as the the primary methodological approach for this research.

Interpretivism, on the other hand, enables understanding complex socio-technical phenomenons like the use of electronic identity schemes on the national and cross-border scale [83]. According to interpretivism, reality cannot be explained without understanding social actors in it [109]. Therefore, the author is guided by interpretivism, especially in the first part of the research, when it was essential to understand the stakeholders, their roles, and their interrelations on the national and EU level together with the legal framework.

Combining those two paradigms enables a broader approach to the research topic. Moreover, the author applies inside the design science paradigm the methods such as case study [182] to understand particular social phenomenons related to the electronic identity (i.e., normative environment, stakeholders, users, etc.). When pragmatism was a suitable paradigm for design science [51], then interpretivism matched well with the case study methodology [109].

Finally, the author proposes an assessment framework for eID schemes based on the input collected during the research. Triangulation of data and theories ensures a versatile approach to the research question [47]. Section 2.2 gives a more detailed overview of the applied research methodology.

2.2 Research Methodology

This research follows the design science (DS) research methodology [60]. The design science paradigm is oriented to problem-solving and originated from engineering [60] and the sciences of the artificial [133]. Current research tries to solve the interoperability challenge in the field of eID by proposing an assessment framework for eID schemes´ cross-

border use. DS research guidelines give a clear path to meet the research goal. Therefore, the author selected DS as the primary research methodology for this dissertation.

The author admits that the DS methodology is information systems (IS) discipline centric. However, according to the DS, the research artifacts can be "constructs, models, methods or instantiations" [60]. The DS framework design can refer to a process and a product [60]. The proposed eID schemes assessment framework (an artifact of this research according to DS) offers one method to identify whether the eID solution corresponds to a certain assurance level. During the design process, the author analyses existing peer review process and other sources and proposes the assessment framework.

Information systems are not independent units but are influenced by organisational structures where they are implemented. Therefore, it is essential to combine DS research with the elements from behavioral science supported by theoretical institutional design framework [80, 60]. Fig 2 presents the DS framework in combination with the behavioral approach proposed by Hevner, March, Park, and Ram [60]. The environment consist of people, organisations, and technologies. Therefore, the author focused in the first part of the research on the national eID practice analysis, eID stakeholders and their roles, the eID ecosystem and its components, and user preferences. As the business needs are assessed through the organisational strategies and structures [60], the author analyses eID strategy-building process separately.

The behavioral approach relies on the development and justification in the research [58]. Analytical and experimental methods, case and field studies, and simulations are applicable within behavioral science [179, 60]. Therefore, the author has used case study methodology in several research activities. A detailed overview of the used methods and data collection procedures is presented in sub-chapter 2.3.

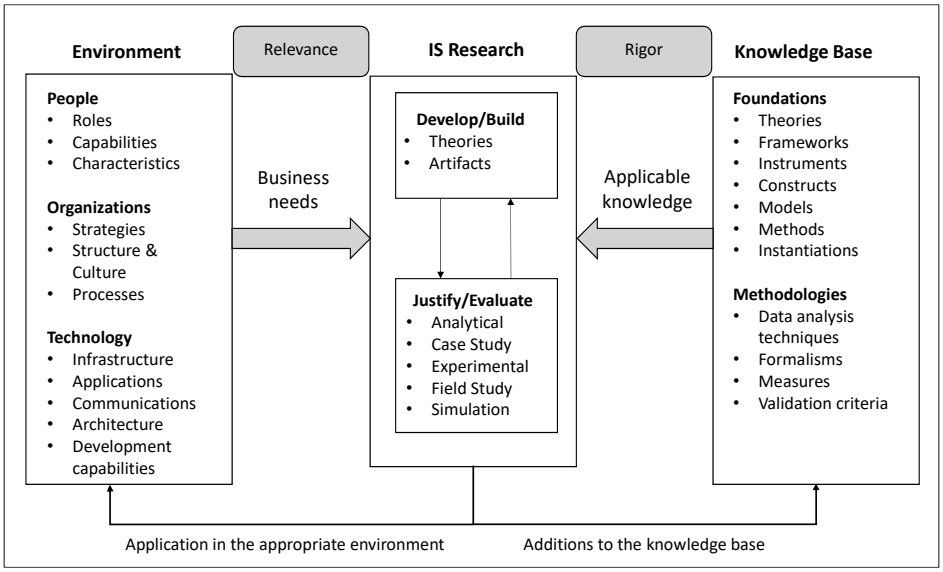

Figure 2: Framework for information systems research by Hevner, March and Park; retrieved entirely from [60] page 80.

DS´s main keywords are building and evaluation [59]. The author designs an artifact following DS guidelines. The evaluation process is described in sub-chapter 2.4. Fig 3 presents the seven-step process of the DS research starting from artifact design and prob-

lem relevance to the final research results communication [60]. Table 2 reflects how the author follows the DS guidelines throughout the research. It has to be noted that the author uses a broader definition of an IT artifact [60]. To demonstrate the study's rigor, sub-chapter 2.3 focuses in-depth on the data collection and analysis description, and sub-chapter 2.4 provides an overview of the validation procedures used for this research.

No	Guideline	Description
1	Design as an artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
2	Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
3	Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
4	Research contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
5	Research rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
6	Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7	Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Figure 3: DS research guidelines by Hevner, March and Park; adapted from [60].

2.3 Data Collection and Analysis

Within this research, it is possible to distinguish three data collection rounds. Fig 4 presents the data collection stages and used data collection methods in each step. Data collection in the first stage focused on the data related to the national eID practices and addressed the SRQ1. In the second stage, the author analysed the data related to the EU level and eIDAS regulation implementation practice answering the SRQ2. In the third stage, when designing the assessment framework, the author analysed legislation, standards, and other documentary sources and conducted semi-structured interviews with the CN experts addressing the SRQ3. Chapter 7 provides an overview of the qualitative interview results from the third data collection stage. It has to be noted that some publications of the author help to answer more than one SRQ.

2.3.1 First Data Collection Stage

The first data collection stage included several research activities focusing on different aspects of the national eID practice. Table 3 gives an overview of the research methodologies and data collection procedures used in the first data collection stage. The case study was mainly used as a methodological approach (in seven research actions). The author used an approach oriented toward action design research (ADR) in two cases. The data was collected in qualitative and quantitative ways. The author analysed the legislation and other documents (L/D), conducted interviews (I), and reviewed existing literature

Table 2: Application of DS guidelines

Guideline	Application
(1) Design as an Artifact	As a result of the research, a multifaceted framework for the eID schemes assessment is proposed.
(2) Problem relevance	The objective of the research is to create a multi-faceted assessment framework for eID schemes to enable their cross-border use.
(3) Design evaluation	Designed artifact is rigorously evaluated using scenario-based method [60] and expert interviews.
(4) Research contributions	The contribution is artifact itself that can be practically used in the eID schemes assessment process.
(5) Research rigor	The author has applied rigorous methods as case study, action design research (ADR), qualitative and quantitative research methods throughout the design process. Descriptive method is used for the DS evaluation.
(6) Design as an search process	The author analyses various sources (legislation, standards, work processes, theoretical concepts) to solve the research problem.
(7) Communication of research	The research results are presented at the PhD defence and reflected in the author´s publications. The author plans to present the results at the CN meeting

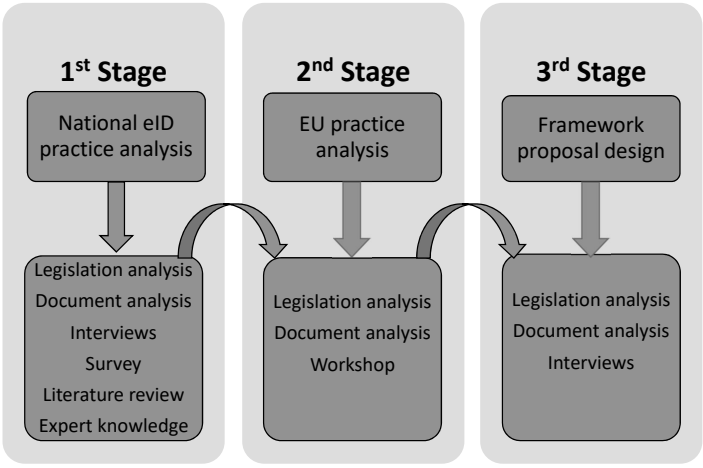

Figure 4: Data collection during the research.

(LR). eID user perspective is reflected through survey (S) results. In this case, the author helped to design the survey questions and contributed to the research design. The author has worked in parallel as a practitioner in the eID domain at the Estonian Police and Border Guard Board (PBGB) and the Information System Authority (ISA). Moreover, the author is a member of the CN. Therefore, the research papers also include expert knowledge (EK) from practice.

Publications VI, V, XII and IX cover eID legislation analysis on the national level

Table 3: Methodology and data collection - national eID practice (SRQ1)

Pub No	Methodology	L/D	I	LR	S	EK
I	Action design research		x	x		x
V	Action design research	x	x			x
VI	Case study	x				x
VII	Case study				x	
VIII	Case study				x	
IX	Case study	x				
X	Case study		x	x		x
XI	Case study		x			x
XII	Case study	x	x	x		

(L/D) - legislation/document analysis; (I) - interviews; (LR) - literature review; (S) - survey; (EK) - expert knowledge.

based on Estonian example. In addition to the juridical documents, the author analysed international standards, guidelines, strategic documentation and development plans. In case of publication IX, the author broadened the scope rather than eID and analysed e-governance related normative acts and their dependencies. Data was collected using official websites of government authorities. Legislation data was collected using Estonian official legislation database Riigi Teataja[1].

The first data collection stage contained four different interview rounds. To understand the national eID strategy, stakeholders, and roles, the author conducted twelve individual non-standardized interviews [31] with Estonian public and private sector representatives closely related to the eID field. Interviews were recorded, transcribed, and thematically analysed [23]. More detailed overview of the data collection and analysis of these twelve interviews is described in publications I and V.

Data exchange framework and national interoperability architecture and implementation practice are analysed in publication XII. Ten experts were interviewed from different countries having x-road implementation experience. Interviews were recorded, transcribed, and thematically analysed using NVivo software [39]. A more precise procedure is provided in publication XII. It has to be noted that in this research activity, the author was not the one who conducted the interviews but helped to present the research results.

eID´s national perspective included also security, risks, and incident management. Publication XI presents how Estonia handled in 2017 security vulnerability called Return of the Coppersmith's Attack (ROCA). The study is based on 32 semi-structured interviews with 41 individuals (including the author of the dissertation). The Estonian Information System Authority ordered the study from the Tallinn University of Technology (TalTech) [175]. An overview of the thematic analysis and identified themes and codes is presented in publication XI.

Finally, the author researched Estonian the e-residency phenomenon from the state and entrepreneur´s perspective. e-Residency is a new concept in the field of eID and, therefore, worth a separate study. Twelve semi-structured interviews were conducted (five with public sector and seven with private sector representatives). The interviews were conducted by the master´s student supervised by the author. The author proposed the research design, helped form the interview questions, and analysed the data. Data collection and analysis details are available in the publication X.

[1]www.riigiteataja.ee

In the framework of publications I, XII and X, literature reviews were conducted. eID user preferences and factors affecting the eID public acceptance were studied via an online survey. Two hundred sixty-eight respondents holding at least one of the Estonian eID means took part in the online survey created using the surveymonkey.com platform. The author helped to design the research and survey questions. Overview of the survey design and results are presented in the publications VIII and VII.

To sum up the first data collection phase, the research results contain input from 66 qualitative interviews and feedback from 268 online survey respondents together with detailed Estonian e-governance legislative environment and other related documents (guidelines, standards, strategies, etc.) analysis, three literature reviews and author´s expert input from practical work experience.

2.3.2 Second Data Collection Stage

The second data collection phase focused on the European Union practice analysis and eIDAS regulation implementation. Table 4 gives an overview of the research methodologies and data collection procedures used in the second data collection stage. The author uses action learning and case study research methodologies in the second data collection stage. The data was collected using mainly qualitative methods. The author analysed EU legislation and other eID-related documentary sources, provided a literature review, and conducted a workshop to identify the eIDAS regulation implementation challenges.

Table 4: Methodology and data collection - EU practice analysis (SRQ2)

Pub No	Methodology	L/D	EK	LR	WS
II	Case study	x	x	x	
IV	Action learning	x			x
XIII	Case study		x		x

(L/D) - legislation/document analysis; (EK) - expert knowledge; (LR) - literature review; (WS) - workshop.

The author identified challenges related to the eIDAS regulation implementation by comparing the Estonian and the Netherlands practices. The author conducted a two-day workshop between experts from both countries. On the first workshop day, the experts mapped eIDAS-related challenges. On the second day, we focused on finding the solutions to the previously mapped challenges. The author facilitated the discussions and participated as an expert in the workshop activities. After the workshop, the author digitized the workshop materials and presented the findings and detailed workshop description in the research paper IV.

This two-day workshop was part of a larger collaboration project conducted on 18.11-21.11.2019 in Tallinn. The author was one of the main organisers of the event. In addition to the eIDAS implementation challenges, development of data exchange infrastructures of Estonia and the Netherlands was researched. The results and research design are presented in publication XIII.

eIDAS regulation revision triggered the need to analyse the latest developments related to the eIDAS regulation. From the research perspective, it was essential to understand stakeholder´ expectations and the EC´s political directions. Therefore, publication II presents a summary of the public, private, and academic sector feedback and expectations towards the eIDAS regulation submitted during the public consultation procedure launched by the EC. 156 pages of material were thematically analysed, and the results were compared with the revised eIDAS regulation proposal presented by the EC.

Publication II describes the exact data collection procedure together with the literature review and comparative juridical analysis.

The second data collection stage results include four-day workshop materials held between Estonia and the Netherlands, eIDAS regulation development and implementation analysis, and 156 pages of eIDAS regulation feedback from the stakeholders.

2.3.3 Third Data Collection Stage

The third data collection stage enables answering the SRQ3 and provides direct input to the eID assessment framework design process. Table 5 gives an overview of the research methodologies and data collection methods used within the third data collection stage. These works from previous data collection stages directly support the outcome of the dissertation. In addition to the publications mentioned in table 5, the author has conducted a literature review of eID and eIDAS-related work (presented in chapter 3) and analysed existing eID peer review routines in the EU (presented in chapter 6).

Table 5: Methodology and data collection - framework proposal design (SRQ3)

Pub No	Methodology	L/D	I	LR	WS	EK
II	Case study	x	x	x		
IV	Action learning				x	x
V	Action design research	x	x			x
XIII	Case study				x	x

(L/D) - legislation/document analysis; (I) - interviews; (LR) - literature review; (WS) - workshop; (EK) - expert knowledge.

To understand practically how member states recognise the eID schemes of other countries, the author of this dissertation conducted ten qualitative semi-structured interviews with eleven CN experts from nine European Economic Area (EEA) countries. The main aim was to understand the actual working process and obstacles in the current working process. Table 6 provides an overview of the interview participants and their country of origin. The interviewees were selected based on their active participation in the peer reviews and availability. Active participation means that the CN member has participated as an active member and/or has been a coordinator or rapporteur at least in two peer reviews in the last two years.

Participation in the peer review process is voluntary, and some CN members do not choose any role in the peer review process or take part only as observers. Therefore, these CN members were not considered as a target group of the interview.

The duration of the interview remained approximately 40 minutes up to an hour. The interviews were conducted using MS Teams or Skype for Business online platforms. The interviews were recorded, transcribed, and analysed using NVivo qualitative data processing software[2]. The author conducted thematic analysis following the qualitative data analysis steps identified by Creswell [31]. Fig 5 presents the Creswell data analysis model, slightly modified for this research by the author. First, the author transcribed the interviews and then organized them for further processing. The author read the whole material and coded the text using NVivo software. Then, the author identified the main themes and descriptions from the expert interviews and finally interpreted the results. Data accuracy was validated through triangulation of different data sources [31].

The interview results give practical input to the eID assessment framework design.

[2]https://www.alfasoft.com/en/products/statistics-and-analysis/nvivo.html

Table 6: Interview participants

Name of the Organization	Country	No of Interviewees
Information System Authority (ISA)	Estonia	1
Secure Information Technology Centre (A-SIT)	Austria	1
Ministry of the Interior	Czech Republic	1
The Federal Office for Information Security (BSI)	Germany	2
Agency for Digital Government	Denmark	1
Kirei - Information Security	Sweden	1
Federal Public Service Policy and Support (BOSA)	Belgium	1
French National Cybersecurity Agency (ANSSI)	France	2
Logius – Ministry of the Interior and Kingdom Relations	The Netherlands	1

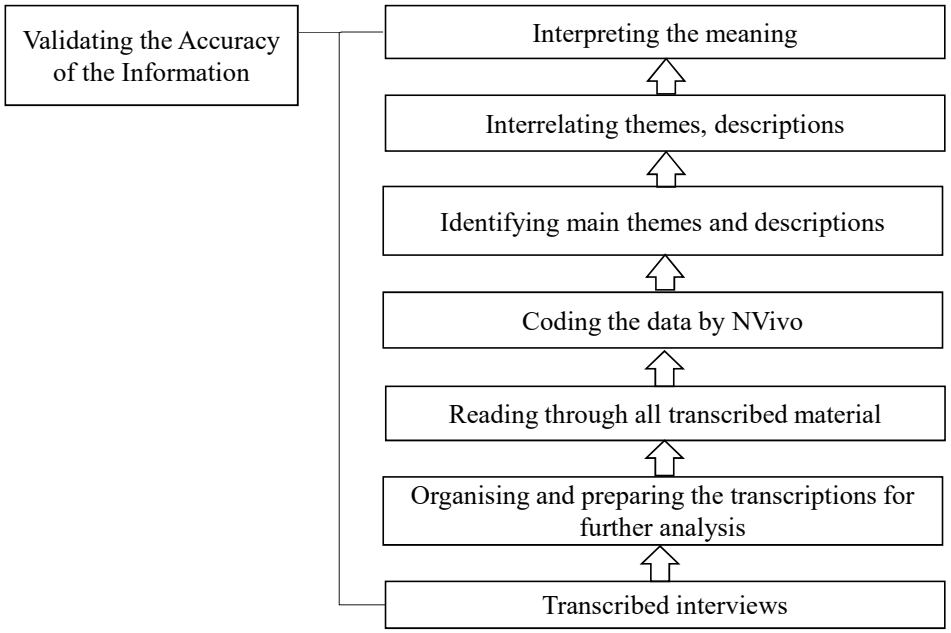

Figure 5: Data analysis model. Source: Creswell model [31] modified by author.

The interview results are presented in chapter 7, and they will be used, together with other data sources (legal and documentary texts, standards, guidelines, etc.), in the eID assessment framework proposal.

2.4 Validation Procedure

According to the DS, the quality of the artifact shall be rigorously presented using a suitable evaluation method [60]. Quality can be evaluated from different perspectives (e.g., functionality, usability, performance, etc.) or how the solution serves the organization's interests where it was implemented [60]. It is essential to understand if the designed solution, method, or framework is applicable in a particular business environment. The quality is achieved when the artifact meets the initial expectations and requirements and can solve the problem for what it was designed [60].

In this research context, the designed assessment framework needs to enable effective evaluation of the eID schemes. It has to be possible to identify if the eID scheme corresponds to a certain assurance level and whether it is secure for cross-border use. According to the DS, suitable evaluation methods include observations, analytical, experimental, and descriptive methods, and testing [60]. Fig 6 gives an overview of the possible evaluation methods in the DS research.

Nr	Method	Description
1	**Observational**	Case study: study artifact in depth in business environment.
		Field study: monitor use of artifact in multiple projects.
2	**Analytical**	Static analysis: examine structure of artifact for static qualities (e.g., complexity)
		Architecture analysis: study fit of artifact into technical IS architecture.
		Optimization: demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior.
		Dynamic analysis: study artifact in use for dynamic qualities (e.g., performance).
3	**Experimental**	Controlled experiment: study artifact in controlled environment for qualities (e.g., usability).
		Simulation – execute artifact with artificial data.
4	**Testing**	Functional (black box) testing: execute artifact interfaces to discover failures and identify defects.
		Structural (white box) testing: perform coverage testing of some metric (e.g. execution paths) in the artifact implementation.
5	**Descriptive**	Informed argument: use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact´s utility
		Scenarios: construct detailed scenarios around the artifact to demonstrate its utility.

Figure 6: Evaluation methods according to DS. Source: Hevner, March, Park, Ram [60].

While choosing the evaluation method, the author reviewed five DS artifact evaluation methods described in fig 6. The author had to take into account the following limitations:

- eID scheme peer review process is time-consuming and can take together with the pre-notification process up to 6 months;
- eID scheme peer review process engages various parties from different countries;
- eID peer review has to be carried out following the EU legislation and according to the agreed guidelines.

Considering the limitations, it was impossible to perform evaluation activities during the peer review process. Therefore, the author conducted two evaluation activities: initial evaluation using expert interviews and scenario-based evaluation.

Moreover, the author found that descriptive evaluation, more specifically, the scenario-based evaluation method, best suits this research. Illustrative scenarios are one of the most commonly used methods in DS evaluation [115]. The scenario-based evaluation method enables evaluating the suitability of the designed artifact based on the scenarios constructed according to the conducted peer reviews.

Therefore, the author described three scenarios for the evaluation based on the peer reviews of Denmark (peer review conducted in 2022), the Czech Republic (peer review conducted in 2021), and the Netherlands (peer review conducted in 2022). Those countries were selected because they reflect the most recent peer review practice (peer reviews conducted in 2021/2022), and selected eID schemes cover levels of assurance "substantial" and "high". In addition, chosen schemes contain technological components that made the peer review of a scheme more challenging.

Scenario-based evaluation helps to understand if the framework is practically applicable and provides additional feedback about the quality of the designed solution. The design artifact is evaluated ex post [119]. Detailed evaluation process and selected scenarios are described in chapter 10.

To increase the inner validity of the proposed framework, the author conducted three additional interviews with the CN experts, who participated in the assessment framework designing process. Through the interviews, the author wanted to understand whether the drafted framework is applicable in real life. Moreover, the interviews gave valuable feedback to improve the initial framework. The author changed the initial framework draft proposal based on the interviewees' feedback. The final version of the eID assessment framework (eIDAF) is presented in Chapter 8. A detailed description of how the interviews were conducted is described in Chapter 9.

3 Related Work

This chapter provides an overview of the eID-related work published in English relevant to this research context. The author used a Google Scholar search engine to identify the eID-related work. The following keywords were used for the search: "electronic identity" (4 210 000 matches), "electronic identity Europe" (2 280 000 matches), and "eIDAS" (4960 matches). Due to a large number of matches, the presented related work reflects a selection of scientific works published in the past ten years, from 2012 to 2022, focusing on the European eID domain. The author considered only electronic identification and authentication schemes related work as a part of the overview. The related work overview does not contain research papers written or co-authored by the author of this dissertation.

Related work is divided into three sub-chapters, starting from the general overview of the eID-related work in sub-chapter 3.1, followed by the eIDAS-related research papers in sub-chapter 3.2 and finally presenting eID case studies of EU member states and European Economic Area (EEA) countries in sub-chapter 3.3. It is important to emphasize that the aim was not to conduct a literature review or a systematic literature review [76] but give a thorough insight into the eID-related research papers in an organised way.

3.1 General eID Related Work

It is possible to find many electronic identity-related research papers with the EU focus published in the past ten years. For example, a study from 2012 analyses interoperability projects carried out since 2004 and provides an overview of the trends in pan-European identity management systems [145]. However, the field itself is complex and interdisciplinary. Van Dijck and Jacobs emphasise that electronic identity field development is more than just technical and juridical aspects but also comprises discussions over the contradicting social and political values [176]. Based on the search results, the academic works inside the general framework can be divided into three main categories: research papers focusing on eID legal aspects, technology and eID infrastructure-related work, and research papers analysing concrete use cases or business processes. Chapters 3.1.1, 3.1.2, and 3.1.3 summarise the general eID and eIDAS-related work from different perspectives.

3.1.1 Legal Perspective

This sub-chapter focuses on academic works conducted in the EU eID field from a legal perspective. Directly eIDAS regulation-related research papers are not included but presented separately in sub-chapter 3.2. Research papers focusing on a particular EEA country eID and eIDAS implementation practices are analysed in Section 3.3.

Electronic identity is one of the essential building blocks of the European Digital Single Market. Schmidt, Krimmer, and Lampoltshammer present the results of a study in the framework of a Single Digital Gateway Regulation (SDGR) showing relations and dependencies between the eID and Once-Only Principle (OOP) [127].

Some of the works focus more on the development aspects of the eID and identity management-related legislation. Sullivan gives a general overview of how the digital identity legal concept has evolved over time [144]. Iglezakis analysis in his paper the legal aspects of electronic identity management systems based on the EU legal framework [63]. De Andrade has conducted an in-depth study on the EU eID legislative and regulatory aspects [11]. He analysed the EU electronic identity legislation and found that despite the technological capabilities, the legal interoperability in the field of eID is missing [36]. He also pointed out in 2012 that the legislative framework for pan-European electronic identity is not sufficient [10]. De Andrade also analysed the EU eID legislation in the context

of the Lisbon Treaty [35]. In the later work, de Andre, Monteleone, and Martin present their project results about the European electronic identity and related legal challenges and future perspectives [9]. However, it must be noted that de Andrade's works were all carried out before the eIDAS regulation came into force.

Other works go beyond and analyse the legal aspects on a constitutional level. For example, De Gregorio approaches the eID juridical aspects more generally.He provides an approach to the EU's policy shift and states that the EU has entered from a liberal economic era to the phase of digital constitutionalism that challenges the EU constitutional law [37].

Privacy and data protection topics are closely related to electronic identification and legislation. A report from the year 2012 presents the results of a pan-European study about people´s attitudes and preferences regarding the eID together with privacy and data protection matters [93].

Some of the research papers focus on the legal practices of certain European Countries or regions. For example, Lentner and Parycek compare authentication and identification-related legal practices of Austria, Germany, Liechtenstein, and the Swiss Canton of Zug [85]. They found that every country has adopted a different legal approach to electronic identity due to the different juridical practice and existing legislative environment [85]. Hansteen, Ølnes, and Alvik provide a survey-based overview of the eIDs in Nordic countries (Denmark, Finland, Iceland, Norway, Sweden), including the legal environment analysis and improvement proposals [56].

In addition to the concrete legal case studies, it is possible to find juridical works focusing on technology trends in the EU, such as artificial intelligence (AI) implementation and cloud computing. Electronic identity legal aspects are analysed within the study that aims to identify the EU laws related to digitization and, more specifically, in relation to AI [30]. Sädtler discusses identity management legal aspects in the context of cloud computing [122].

3.1.2 Technology and Infrastructure

Many works focus on the technology and infrastructure aspects of eID and eIDAS. Some works are related to the governments provided electronic identities, and some works provide alternative or combined solutions to the existing electronic identity schemes. One of these examples is a FutureID project that aims to address the interoperability challenges within the European Union (EU) by developing an environment that enables integration of the eID technologies on the back end [121]. This project aimed to create a decentralized identity management ecosystem for the EU [24]. One published work in the FutureID project framework also discusses the need for interdisciplinarity in technical projects and the practical use of the design science research methodology [131].

Lenz and Zwattendorfer propose an eID architecture based on modular and plug-in approach [86]. Another study proposes an architecture for the European eID system based on federated identity and analyses its performance and scalability [28]. Zefferer, Ziegler, and Reiter combine cloud computing and eID and propose a solution that integrates EU and national systems, enabling secure cloud federations [186, 185].

Garcia, Oliva, and Pérez-Belleboni analyse the practice in electronic identity management (eIDM) systems at the pan-European level [48]. One of the studies presents the results of extensive eID usability and interoperability research conducted by the SSEDIC (Scoping the Single European Digital Identity Community) thematic network [147, 81]. According to this research, the primary key areas in digital identity management are "mobile identity, attribute usage, authentication, and liability" [147].

Mobile-based eID solutions are becoming more and more popular. This is also illustrated by the fact that there are many works available focusing on the mobile ID solutions. Zefferer and Teufl analyse existing mobile ID and signature solutions in the EU and propose how to implement those solutions more efficiently [184]. A study from 2014 focuses on mobile identity management and provides an overview of the mobile identity implementation cases in EU countries [5]. Houdeau has analyzed sixteen European electronic identity programs based on two-factor authentication in the framework of the EU Digital Agenda [61]. Massoth proposes in his research paper a two-factor authentication solution using near-field communication (NFC) technology in combination with the German eID card [99]. Research paper about the My Identity App (MIA) presents a platform-independent mobile application-based electronic authentication solution embedded in an eID ecosystem [149].

In addition to the mobile-based technologies, some of the latest publications study possibilities to integrate blockchain technology into the eIDAS framework [55, 82].

3.1.3 eID Use-Cases

Based on the literature, it is possible to distinguish three main eIDAS implementation use cases: the educational, healthcare, and banking/finance sectors. There are also some other use cases. For example, one research paper presents practical cases of using eIDAS for Login and Wi-Fi access [20]. However, their importance and volume are not even comparable to those works conducted in those three domains.

eIDAS implementation in the educational sector is one of the most researched use cases. The research papers attempt to integrate new technological approaches with the eIDAS framework or focus on a particular use case. Moreover, some academic research papers present findings about sharing additional attributes within the eIDAS framework. For example, one of the studies proposes the establishment of an European academic identity based on the Self-Sovereign identity (SSI) technologies [74]. Some research papers present a concrete use case of integrating particular e-governance solutions (like the German eID card, the eGovernment Protocol OSCI, etc.) into the existing university management systems [138, 141, 139, 140]. One of the studies focuses on the eIDAS implementation in shared learning environments [78, 79]. Italian study presents a case where the university and the banking sector launched an UniCam card enabling users access to their bank accounts, university services, and the possibility to give a digital signature [46]. Similar studies were conducted in Greece to integrate educational services with the national eIDAS node [49, 95]. Berbecaru, Lioy, and Cameroni describe an approach based on eIDAS infrastructure that enables attribute sharing in academic services [19]. One study focuses on the "eID for University" (eID4U) project as a practical case of implementing eIDAS in academic services [17]. Another research paper presents the extension of the Spanish eIDAS infrastructure in academic attributes sharing [7].

Healthcare is another eIDAS use case example. Patient identifier is an important unit for the provision of cross-border e-health services. Therefore, researchers have analysed current attribute-sharing practices to enable the exchange of patient identifier information [137]. One of the studies focuses on using eIDAS-compliant national eIDs for the cross-border healthcare data exchange [73].

Online banking is one of the cornerstones of digital service provision. According to one study, EU digitization and datafication main pillars (including digital identification systems) lead to data-driven finance [187]. Therefore, banking and other financial services form one of the eIDAS implementation use cases. For example, one of the research papers presents the survey results conducted by European Union Agency for Cybersecurity (ENISA) focus-

ing on the financial sector and related security issues assessing known threats in the eIDAS implementation context [177]. In addition, one of the works focusing on the financial market is presented in sub-chapter 3.2.

3.2 eIDAS Related Work

This sub-chapter overviews the works directly related to the eIDAS regulation. Some described works remain more on a general level and provide an overall review of the main identification and trust-related concerns in the eIDAS regulation [102]. Other research papers discuss mutual recognition and interoperability aspects of electronic identities [12] and technology, privacy, and data protection concerns.

Berbecaru, Lioy, and Cameroni focus in the eIDAS regulation context on the cases where authorisation is needed before the authentication, and they propose two models for "authorise then authenticate" use cases [18]. From the technical perspective, one of the studies proposes a model enabling connecting FIWARE OAuth 2.0-based services with the eIDAS nodes [6].

With regards to the pan-European eID (EUid), Wagner, Mannino, and Lauer provide an overview of the requirements and main components (including know your customer (KYC) attributes and their LoAs) necessary for designing the EUid from the financial sector perspective [178]. Cuijpers and Schroers analyse eIDAS legal requirements generally relevant in the developing eID schemes in the FutureID project context [33].

Data protection is inevitably related to the eIDAS regulation and its implementation. For example, using pseudonyms is one of the possibilities to reduce the potential misuse of personal data. One of the works addressing, in particular, the pseudonymisation issue found that the eIDAS regulation and EU General Data Protection Regulation (GDPR) [43] approach to the use of pseudonyms is contradictory [170]. Other works stay on a more general level and analyse eIDAS-related data protection aspects from a broader perspective, for instance, evaluating the applicability of the "Data protection by design" principle in electronic authentication cases [171].

Some work focuses more on the eIDAS security aspects. For example, one of the studies focuses on data security concerns in electronic identity management [15]. Another research paper provides a security study related to the eIDAS-compliant authentication schemes [41].

Several research papers focus on the additional attribute-sharing issues within the eIDAS network [21, 97, 103]. Moreover, one of the studies proposes an attribute enabling module (ATEMA) that combines eIDAS authentication data with national layer [16].

eIDAS regulation is researched from the cloud computing perspective. For example, Hühnlein analyses cloud computing techniques to enable providing eIDAS as a service [62]. In addition, some research papers try to combine mobile technologies and cloud computing under the eIDAS framework [69].

A recent study about eIDAS 2.0 and SSI discusses opportunities and challenges regarding the European Digital Wallet and aspects related to the need for standardization [130, 129].

3.3 National eID practices

This sub-chapter provides an overview of the academic works related to the electronic identity schemes of different EEA countries. As a general approach, in the related work chapter, research papers published within ten years were taken into account. However, the ten-year limitation was not applied in the case of national eID practices, as some of the

national eID initiatives were launched much earlier. The author included in the overview only research papers focusing entirely on a particular country's eID practice, as many comparative studies are available. Due to Brexit [29], the author did not consider research papers concerning the United Kingdom (UK) as a part of this overview. After Brexit, the eIDAS regulation was not applicable in the UK. Therefore, the UK adopted eIDAS regulation principles into their national law [108].

Several studies are focusing on Austrian eID. One of the studies, for example, analyses social, technical, legal, and organisational aspects of the Austrian eID [94]. Austrian electronic identity infrastructure is also analysed from the interoperability perspective [148]. Zwattendorfer and Slamanig analyse how the Austrian eID system could be moved to the cloud [188].

Belgium eID card evolution and privacy concerns are thoroughly researched [45, 98]. Bulgarian electronic identity practice is researched in the e-government services context [75]. One research paper describes the basic eID organisation in Croatia [183]. Cyprus eID practice is usually described as a part of larger studies [132]. Špaček introduces eID implementation and selected challenges related to the e-government initiatives in the Czech Republic [136]. A study about the Denmark NemID gives an overview of the cooperation between the Danish government and the banking sector while developing the Danish eID [101]. Another article focuses on social risk analysis during the Denmark NemID implementation [107].

Estonian eID practice is quite well-researched from different perspectives. Some general works describe how Estonian e-government components like PKI infrastructure, data exchange layer X-road and government portal have evolved over time [71]. Other works focus more on the technical and security aspects of the Estonian eID. For example, analysing possible message encryption framework requirements [110] or proposing security improvements for Estonian eID card [114]. Estonian eID card is also analysed in the context of the ROCA (Return of Coppersmith's attack) security vulnerability discovered in 2017 [113]. Electronic voting using the Estonian eID card is also researched [169].

As the Estonian e-residency project was one of the first initiatives of its kind, then some research papers focus on the Estonian e-residency project analysis [126]. Furthermore, the Estonian e-residency project is also analysed in the eIDAS context to determine whether the regulation adds additional value or challenges similar national initiatives [1].

German eID card is widely researched. German eID project is often used as an example to discuss the electronic identity and its infrastructure from an application perspective [117]. At the same time, the German eID card has been criticized from the usability perspective. One of the eID-related studies provides an overview of the lessons learned from the German eID card implementation [135]. In addition, one of the studies analyses the German eID extension proposal by Bundesdruckerei "enabling the protocol to authenticate further transaction data such as phone numbers or PGP keys" [104].

Greek government´s initiative to use eIDs is also analysed from the technical and social perspective [72]. eIDAS regulation implementation in the Hungarian public administration and related challenges are reflected in one of the studies that also proposes two additional registration procedures to complement the missing data items [77]. Lithuanian eID implementation practice in the public sector is analysed in one of the research papers [116].

Grönlund describes the eID implementation practice in Sweden [52]. Rissanen gives an overview of the introduction of the Finnish eID card [120]. There are several works available focusing on the Spanish eID practice. For example, research papers provide an overview of the Spanish eID card implementation [57] and its diffusion [13]. One of the

research papers presents an On-SiteDriverID authentication scheme based on the Spanish eID card [124]. Portuguese practice is analysed in the research paper proposing a secure architecture for an electronic ticketing system based on the Portuguese national eID card [32].

To summarize the national-level eID-related work, it is visible that the eID practices of some countries are more thoroughly analysed than others. For example, Germany, Estonia, and Spain are often used as reference countries. However, the eID practices of some countries were not separately researched, or they were not available in English. For example, the author did not find separate works publicly available in English describing French, Latvian, Maltese, Polish, Irish, Slovakian, Slovenian, Luxembourg, and Romanian eID practices.

4 Theoretical Background

This chapter provides an overview of the theoretical background of the research. The author decided to use identity theory, the institutional design proposed by Koppenjan and Groenewegen, and technology assessment theory. Selected theoretical concepts help frame the research and understand electronic identities, their interoperability, and assessment systematically and comprehensively.

4.1 Identity Theory

Identity is a core component of the eID schemes and their assessment. Therefore it is important to understand the identity concept. Identity theory [25] provides a theoretical basis for this research and helps to frame electronic identity and its relation to the individual and his or her other identities and service providers. Therefore, this sub-chapter focuses on the identity theory analysis in the context of electronic identity. However, it must be noted that this theory focuses more on the social aspects of identity rather than the technical concept of identification. The author analyses the identity theory from the electronic identity perspective and brings out similar patterns on the social and digital levels.

Peter Burke and Jan E. Stets can be considered founders of the identity theory. The concept of identity seeks the answer to a question, who one is [25]. The same question becomes essential in the e-governance context. Public and private e-service providers want to ensure that the service is provided to the right person. It means that the person who requests the service is the one he or she claims to be. However, it is important to mention that certainty does not have to be always 100%. For example, regarding the eIDAS regulation and its different assurance levels, trust towards the user´s identity can be high, substantial, or low depending on an eID means used for authentication [42].

Fundamental ideas of the identity theory were presented first time in 1966 at the American Sociological Association meeting. It is possible to distinguish three ways to understand the identity [142]. According to one approach, identity refers to the culture of people [27]. Identity can also be seen as a social category [146] or a part of a self-based on the person´s interpretation of his or her different roles in a society [142]. This last concept best matches the current research that considers electronic identity as part of a person´s identity.

More specifically, identity theory tries to explain the concrete meanings people attribute to their multiple identities and how these different identities interrelate to the person and society [25]. The internal self-structure contains multiple identities hierarchically organised by their salience [143]. Based on the identity theory, a person can have several identities. However, something becomes a part of a person´s identity only when a person interprets a particular role as a part of his or her identity, and it is salient enough. Those identities the person commits the most become salient [111].

Considering the general level of digitisation, many individuals' roles in the physical world have moved or duplicated into the digital sphere, which means that people are taking more roles in the electronic environment, and the importance of a digital part of a person's identity increases. This tendency leads to the need to define clearly the digital part of the identity and ensure its connection to the individual. In this case, the electronic identity becomes a salient part of a person's identity.

This reasoning is supported by Jenny L. Davis, who researched the applicability of the identity theory in the digital transformation era. Davis focuses on the situations and implications of online connectivity [34]. According to the identity theory, a situation triggers

the person´s identity [34]. For example, a teacher activates his/her teacher identity at school. Based on that example, a person´s digital identity is activated when using a digital environment. Davis discusses that even in digital environments, individuals activate their different identities (e.g., in different social media platforms or depending on an open or closed online group) [34]. A similar pattern can be noticed when people interact with government authorities or private sector service providers using their electronic identity. In this context, the particular form of eID, the subject of this research, is just one reflection of the person´s multiple digital identities. In other words, electronic identity as a unique set of attributes enabling the identification of the person in electronic environments, is one part of the person´s identity.

When a particular identity (e.g., electronic identity) is clearly formed, it will be maintained through continuous verification. It means that a person compares his/her understanding of the identity with the feedback received from the situation where the identity was activated [34]. This kind of identity confirmation loop seems to take place on the individual and collective level. E-service providers try to ensure the continuity of the person´s identity in the digital environment via different verification procedures and requesting various attributes related to the person. In parallel, the person keeps verifying his/her digital identity by receiving feedback for his/her digital actions.

Understanding a person´s multiple identities and their verification mechanism leads to the next step, where it is possible to investigate the electronic identity concept more closely through different institutional layers.

4.2 Institutional Design by Koppenjan and Groenewegen

The eID schemes operate nationally and internationally and are complex socio-technological constructs to research. However, complexity, in this case, does not mean that the technological solution itself is complex. Instead, eID ecosystems contain multiple interrelated layers to be fully operational. According to Koppenjan and Groenewegen, complex technological systems have certain specific characteristics [80]. Table 7 illustrates how eID systems correspond to the characteristics of complex technological systems. Based on the table, it is evident that eID schemes meet all criteria and can be considered as subjects of institutional design [80]. Therefore, the author decided to use the institutional design proposed by Koppenjan and Groenewegen to understand more deeply and systematically how the technological and institutional aspects of eID systems interrelate.

Complex technological systems presume institutional design that helps to manage the relations between the parties operating the system [80]. According to Koppenjan and Groenewegen, complete design process forms in relation to the technological, institutional, and process design as presented in Fig. 7 [80]. Process design focuses on the parties involved in the design process, conditions, and rules that must be followed during the process etc [80]. Technological and institutional design are outcomes of a process design, tying technology systems and their components together with normative environment [80]. "Institutions regulate behavior and are essential components of socio-technical systems" [22].

In the context of eID, the process design consists of various public (ministries and other authorities) and private (certification service provider, eID mean manufacturer, personalisation service provider, etc.) sector stakeholders, as well as standards applicable in the eID field and national and EU level strategies, working documents, guidelines, etc. that need to be taken into account in the design process. eID technological design contains components like PKI infrastructure, an x-road data exchange layer, eIDAS Nodes at the EU level, etc. The institutional design consists of legal regulations applicable in the field of

Table 7: eID as a complex technological system

Characteristics	eID schemes
Technological component is important but it does not determine individually the system operation	eID schemes rely on technology, but it is only one part of the whole ecosystem. eID ecosystem is supported by numerous administrative and organisational processes and influenced by users and service providers.
Involves multiple parties	eID ecosystem engages multiple actors. For example, already from the public sector perspective, different ministries and authorities (PBGB, ISA, etc.) are involved in the eID ecosystem management.
Public and private parties involvement	eID ecosystem is operated in cooperation with public and private sector parties and is actively used by both sectors.
Influenced by market forces and government regulations	The market influences eID ecosystems as they contain services (trust services, helpdesk services, etc.) and products (tokens, chips, software, etc.) subject to public procurement. eID field is regulated on the national and EU level.

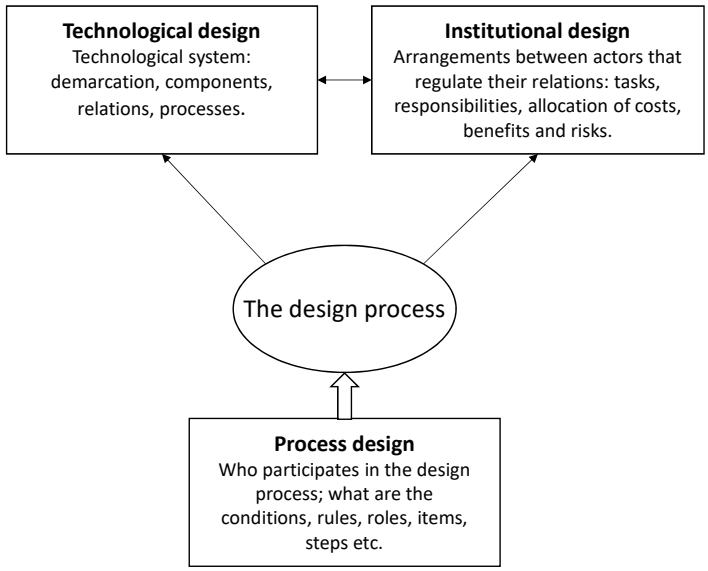

Figure 7: Positioning of institutional design by Koppenjan and Groenewegen [80].

eID and its related domains on the national (eID-related laws, procurement law, cyber security regulations, etc.) and EU level (eIDAS and its implementation acts, SDG regulation, etc.). Therefore, the institutional design of the eID schemes can be viewed separately at the national and the EU level. Fig. 8 presents the two-layer institutional design of eID

schemes. The same authorities usually participate in the design process at the national and the EU level. Therefore, national and EU-level technological systems are connected and with the capacity to be interoperable. At the same time, national and EU institutional design components are intertwined through policy-making, cooperation, and legislative process.

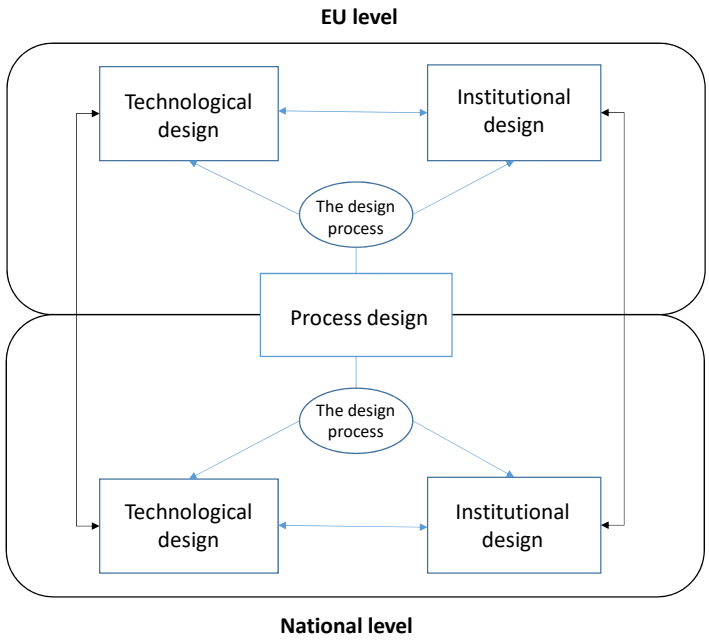

Figure 8: Institutional design of eID schemes based on the Koppenjan and Groenewegen [80].

To understand complex-technological systems better, Koppenjan and Groenewegen introduce a four-layer model for institutional analysis [80]. Their proposed model is based on the models Oliver Williamson developed in the field of economics [180, 181]. However, Koppenjan and Groenewegen have developed the concept further by adding actors and strategies to the model and enabling interaction between different layers [80]. Fig 9 presents four levels of institutional analysis proposed by Koppenjan and Groenewegen.

The first layer includes "actors/agents and their interactions aimed at creating and influencing (infrastructural) provisions, services, outcomes". The second layer forms from "gentlemen agreements, covenants, contracts, alliances, joint-ventures, mergers, etc. and at the informal level rules, codes, norms, orientation, relations" [80]. The third layer contains "formal rules, laws, and regulations, constitutions, (formal institutions)," and finally, the fourth layer covers "norms, values, orientations, codes (informal institutions, culture)" [80].

Based on the four-layer model of Koppenjan and Groenewegen, it is possible to analyse the eID ecosystems. On the national level, table 8 presents the institutional design of the eID ecosystem from the national perspective. The national model is based on the Estonian eID environment, describing actors and formal and informal environments.

At the same time, the eID ecosystems' institutional design can be described at the EU and EEA levels. Table 9 illustrates the institutional design of the eID schemes at the EU/EEA level, adding international and interoperable dimensions to the national view.

From the challenges point of view, Koppenjan and Groenewegen bring out that chang-

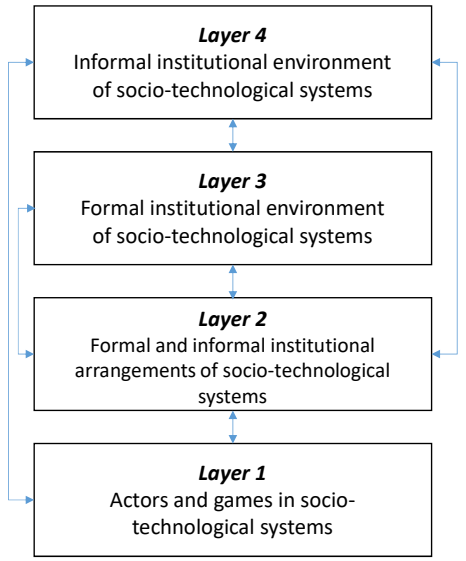

Figure 9: Levels of institutional analysis by Koppenjan and Groenewegen [80].

ing complex technological systems is a challenging task as these systems engage several parties/stakeholders, and technical systems cannot be operated independently from the organisational environment [80]. Therefore, it is essential to consider all four layers in the institutional design [80]. This dissertation follows the four-layer institutional analysis model proposed by Koppenjan and Groenewegen to describe and understand the eID ecosystem in the national and EU context.

4.3 Technology Assessment

In the eID schemes peer review process, member state experts often face the challenge of deciding if the presented solution is secure enough and suitable for cross-border use on a requested assurance level. When the eID scheme is based on the Public Key Infrastructure (PKI) solution, it is quite easy to decide, which is well-known to experts. However, as technology develops and users´ needs change, experts often have to decide whether a particular eID scheme or a technological component is appropriate for interoperable use. Good examples, in this case, are fully remote identification solutions (e.g., remote video identification solutions, etc.), mobile applications, or cloud-based solutions. Therefore, the author decided to look into the Technology Assessment (TA) approach to strengthen the theoretical basis of the research and add value to the proposed assessment framework.

Technology assessment (TA) is a scientific approach developed in the 1960s and 1970s in the United States (US), and it is used to evaluate the conditions and consequences related to the technology implementation [54]. TA is an interdisciplinary concept addressing the challenges between society and the use of technology [53]. TA is not a technical concept but oriented to the political and social aspects. TA is preventative in nature and gives decision-makers valuable input about possible negative scenarios arising from the use of technology [53]. Therefore, it is a suitable approach from the eIDAS regulation perspective.

When it comes to the new technologies and their acceptance, TA focuses on the pos-

Table 8: Institutional design of the eID ecosystem on the national level. Source: Entirely taken from the publication XI

Layer	Estonian eID ecosystem
Layer 4: Informal institutional environment	People trust government and public sector institutions responsible for the eID ecosystem and provision of e-services [105]. Work attitude and incentives to contribute.
Layer 3: Formal institutional environment	Estonian eID ecosystem relies from European Union side on the European Parliament and of the Council regulation on eID and trust services for electronic transactions in the internal market (eIDAS). On a national level, two main legal acts regulate the eID ecosystem: Electronic Identification and Trust Services for Electronic Transactions Act and Identity Documents Act.
Layer 2: Formal and informal institutional agreements	Underlying principles on technical specifications, ownership, and roles. An essential element of the compulsory roll-out of numerical value for representing the digital identity, Estonian citizens perceive having a digital identity as their right. Identity documents strategy proposed by public and private sector experts. Regular meetings for public and private sector representatives organized by ISA. PBGB and IDEMIA S.A.S. have concluded a contract for the production of eID cards. Public and private institutions develop the eID area in close cooperation and set strategic goals together [90].
Layer 1: Actors and games	Public (ministries, ISA, PBGB, SMIT, etc.) and private (SK ID Solutions AS, IDEMIA, Hansab, etc.) sector authorities. Indirectly involved stakeholders: banks and telecom companies in the Estonian market that contribute to and benefit the most from the use of eID.

sible side effects that the implementation of a new technology may cause [53]. In the eID schemes context, it is very important to be aware of the possible side effects as the accepted new solutions have cross-border effects. TA is oriented more toward the wider spectrum of technological solutions. However, the TA principles can be used as a part of the eID schemes assessment. The aim is not to fully integrate the TA practice into the eID assessment framework but to analyse what elements could be used for the eID schemes review.

Characteristics of TA include risk assessment, legislation analysis, ethical aspects assessment [112], and systemic approach to the correlations between the technological impact and society [53]. Moreover, TA is innovation-oriented and includes considering alternative options. It has to be noted that TA provides valuable knowledge to the decision-making process, how to handle certain challenges, but does not solve them [53]. Therefore, TA can be seen as helpful while deciding if one technology or part of it is suitable for usage. TA principles go well together with the CN role, as they need to decide if one or another solution is suitable for cross-border use.

On the international level, separate organisations and networks focus on TA-related issues. For example, European Parliamentary Technology Assessment (EPTA) community. EPTA advises governments in TA-related matters, for example, how new sciences and technologies may impact societies, economy, or environment[3]. However, unfortunately, it seems that their actual impact remains relatively modest.

[3]https://eptanetwork.org/about/about-epta

Table 9: Institutional design of the eID schemes at the EU/EEA level. Source: created by the author following the four-layer model by Koppenjan and Groenewegen [80]

Layer	eID Schemes
Layer 4: Informal institutional environment	Social and cultural aspects of the EEA countries. The EU and its institutions working culture and attitude. Cooperation and collaboration between the CN members and knowledge sharing.
Layer 3: Formal institutional environment	National laws of the EEA countries regulate the eID field. EU legislation is applicable in the field of eID, starting from the public procurement rules to the cybersecurity regulations. The most important are the European Parliament and the Council regulation on eID and trust services for electronic transactions in the internal market (eIDAS) and its implementation acts.
Layer 2: Formal and informal institutional agreements	Gentleman's agreements at the CN level and in the eIDAS Technical sub-group, their working practice and guidelines, informal working groups (e.g., Coalition of the Willing (COTW)) and eID-related collaboration projects (e.g., the Nordic-Baltic eID Project (NOBID)). As well as EU digital strategy and initiatives contributing in favour of the EU digital single market.
Layer 1: Actors and games	EEA countries and their governmental authorities are responsible for the country´s eID scheme and involve private sector organisations (e.g., certification service providers, eID means manufacturers, personalisation service providers, etc.) and public and private sector e-service providers.

Since the 1970s, the TA concept has changed over time [53]. In addition to the classical TA concept, other approaches in the TA family focus on different technology assessment aspects like ethics, innovation, and participation [53]. For example, in the case of participative technology assessment, different societal groups are involved in the TA process [70]. Constructive technology assessment (CTA) is another approach developed in the Netherlands that focuses on the design evaluation, development, and technology implementation processes rather than novel technology aspects [128].

In parallel with CTA, the Leitbild assessment concept was developed in Germany, focusing on empirical aspects of technology adoption. According to the Leitbild assessment, technological development can be influenced by socially constructed ideals (like "paperless government," etc.) [53]. Moreover, technological development and innovation-driven thinking have led to the innovation-oriented TA enabling to understand and analyse the social impact of innovative technologies [134].

The aim of the TA is clear, but the question is how to use it in practice. Unfortunately, no uniform TA method can be universally applied [53]. However, TA contains different methods that can be adjusted for the particular use case (TA method toolbox) [38]. These methods include different risk assessment and analysis techniques, simulations, describing scenarios, expert prediction, interviews and discussions, discourse analysis, etc [53]. Table 10 presents an overview of the methods used for the TA evaluation and their potential applicability in the eID schemes evaluation process.

Methods in the table are listed according to the Grunwald [53], and their applicability is assessed through the author's expert knowledge. The author marked the method "applicable" in the table if it can be used in the eID schemes peer review process, and its use may add value. Some methods can be used but do not add value to the process.

For example, the author excluded the use of life cycle analysis (LCA) because this method is more oriented toward evaluating possible environmental impacts. Participation is an essential aspect of the technology assessment. However, consensus conferences and the "Citizens', Juries" method may not be the most suitable for eID schemes evaluation as the evaluation presumes specific expert knowledge. The user's perspective can be covered more effectively through the technology acceptance model [84]. Vision assessment is connected to the rise of nanotechnology and helps to assess futuristic technological visions and concepts [53] and, therefore, not that much suitable for regular work routines.

However, even not all applicable methods may not be reasonable to use all at once during the eID scheme peer review process. Therefore, the author proposes a TA toolbox for the eID schemes based on the TA concept and methods.

Table 10: TA methods and their applicability in the eID schemes evaluation adapted from Grunwald [53]

Method	**Domain**	**Description**	**Applicability**
Risk assessment	Technology	Analysis of technical risks and their evaluation	Applicable
Cost-benefit analysis (CBA)	Economy	Evaluation of technological efficiency	Applicable
Life cycle analysis (LCA)	Environment	Technology impact evaluation on the environment	n/a
Decision-analytical methods	Mixed	Integration of various evaluation methods	Applicable
Consensus conference	Participation	Moderated public debate of 10-15 lay people	n/a
"Citizens', Juries" method	Participation	Technological solution judged by lay people using "common sense"	n/a
Mediation	Problem solving	Using third neutral party in the assessment	Applicable
Vision assessment	Strategy	Assessment of visions communicated in social environment	n/a

The CN forms from the member state eID experts. Therefore, discussion between the experts is a regular working format. However, sometimes it is difficult to achieve consensus in certain technological or procedural aspects. In those cases, the TA toolbox for eID schemes should include the following:

- **expert consensus** - documented discussions between the CN members;
- **risk assessment** - assessment of risks related to the technology, processes, and/or interoperability conducted by the notifying member state;
- **mediation** - engagement of third parties or additional experts in the eID scheme peer review process.

Those three components can be applied during the eID scheme peer review process. In addition, it is possible to include other TA methods on a need basis, for example, in the case of the EU Digital Identity Framework and European Digital Identity Wallet solution assessment.

To summarize the theoretical part of the dissertation, the author believes that due to the rapid development of new technologies and digitization, TA principles and methods should be more visibly integrated into the processes while making decisions over technological solutions.

5 Practical Background

This chapter gives an overview of the practical background information essential for this research. Firstly, the author looks more in-depth at the eIDAS regulation development in the context of authentication schemes. Regarding cross-border authentication and interoperability, it is important to describe the Cooperation Network (CN) role and responsibilities. Finally, the author provides an overview and a short description of the already notified eID schemes.

5.1 eIDAS and eID Schemes

eIDAS is a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [42]. Implementation of the eIDAS regulation is a part of the EU digital single market strategy [162]. The eIDAS regulation aims to strengthen the trust in the EU internal market by providing a general framework for cross-border recognition of electronic identities and provision of trust services [42]. The regulation entered into force in 2014 but was not mandatory for the member states. Fig 10 illustrates the eIDAS implementation timeline starting from its voluntary adoption to the renewed version of the regulation proposed by the EC in 2021 [165]. According to the eIDAS Regulation, voluntary recognition of the member states electronic identity schemes was possible starting from September 2015, and the regulation became mandatory for all member states at the end of September 2018 [89].

Figure 10: eIDAS timeline. Figure from [89].

According to the final provisions of the eIDAS regulation, the Commission had to review the application of the regulation by 01.01.2020 [42]. On 23rd of July 2020, the EC published an Inception Impact Assessment (IIA), "Revision of the eIDAS Regulation - European Digital Identity (EUid)" [166]. According to the IIA, only 58% of the EU population can use their eID across borders. Therefore, the European Commission proposed three scenarios for the eIDAS revision. One of them was introducing a European Digital Identity scheme (EUid) in addition to the existing eID schemes. With the IIA, the EC also initiated a public consultation process to collect the stakeholders' feedback about the eIDAS implementation [166]. As a result, in June 2021, the EC published a proposal to amend the eIDAS regulation and establish a framework for a European Digital Identity [165]. The discussions over the proposal are ongoing, and the European Commission expects to finalize the draft at the beginning of 2023. But as far as the discussions over the eIDAS regulation continue, the member states follow existing procedures and legislation.

According to the eIDAS article 6, when a member state would like to use its electronic identity scheme for cross-border authentication, the scheme needs to be recognised by other member states through the notification process on a certain assurance level [42]. eIDAS article 8 defines three assurance levels of electronic identity schemes - "low", "substantial", and "high" [42]. Table 11 presents the differences between the LoA levels according to the eIDAS article 8 [42]. The main differences between the assurance levels are the degree of confidence in the person´s identity and the difference in applied technical and

procedural measures that reduce the possible misuse of the eID. The minimum technical specifications, standards, and procedures for every LoA are regulated in the eIDAS implementing act [160].

Table 11: Levels of Assurance according to the eIDAS article 8

Level of Assurance	Description
Low	"Refers to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards, and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity" [42];
Substantial	"Refers to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards, and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity" [42];
High	"Refers to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity" [42].

In 2017, Germany was the first to notify their eID scheme under the eIDAS regulation on level "high", followed by Estonia (level "high"), Spain (level "high"), Croatia (level "high"), Belgium (level "high"), Luxembourg (level "high") and Italy (level "high") in 2018 [89].

However, even today, not all EU countries have notified their eID solution for interoperable use, indicating that the implementation of the regulation has not been as successful as expected, even though several working groups and institutions regularly contribute to the eIDAS implementation and development activities. Sub-chapter 5.2 provides an overview of the main stakeholders involved in the eIDAS regulation implementation activities.

5.2 Stakeholder´s Overview

eIDAS regulation and its implementation in 27 member states is a challenging task. Therefore, several formal and informal initiatives have been launched by the EC to make the eIDAS implementation smoother and to ease the cross-border use of the eIDs. The main stakeholders from the eID schemes perspective are the eIDAS Expert Group, the Cooperation Network, and the eIDAS technical subgroup. Fig 11 gives a general overview of

the institutions and their relation to the eIDAS governance. Member state view is not presented in the figure as all those institutions are formed of the representatives of the EU or EEA countries. The European executive bodies Directorates-General (DG) are responsible for the everyday management of different EU policy areas depending on their focus. DG CNECT (Communications Networks, Content, and Technology) is responsible for implementing the EU Digital Agenda [4]. Under this, DG operates:

- eIDAS Committee
- the Cooperation Network
- eIDAS Expert Group

The Committees of the European Parliament help the EC in legislative initiatives. The eIDAS Committee is focused on legislative matters regarding the eIDAS regulation [42]. The eIDAS Expert Group is an informal working group discussing the eIDAS juridical matters and making proposals for the secondary legislation in the eIDAS framework. Moreover, their role is to exchange eIDAS-related good practices of the member states [5].

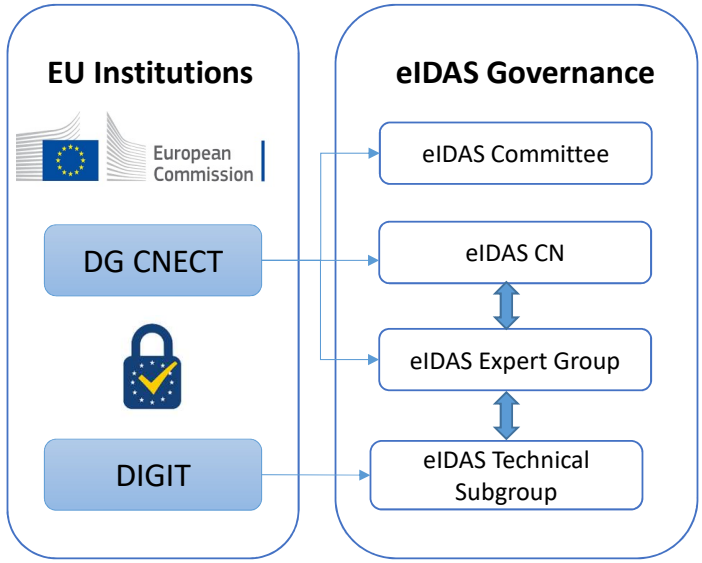

Figure 11: eIDAS stakeholders related to eID schemes.

According to the eIDAS article 12, the EC shall establish the necessary procedural agreements facilitating the cooperation between the member states [42]. For that purpose, the EC established by its implementing decision procedural arrangements for cooperation between member states on electronic identification and formed the Cooperation Network (CN) [158]. One of the CN's responsibilities is to peer review the eID schemes of the member states [158]. Therefore, this dissertation focuses mainly on CN activities. A detailed overview of the CN and its responsibilities is described in sub-chapter 5.2.1.

[4] https://ec.europa.eu/info/departments_en
[5] http://ec.europa.eu/digital-agenda/en/trust-services-and-eid

DG DIGIT (Informatics) focuses on inter-institutional relations and administration [6]. eIDAS Technical Subgroup under the DIGIT is responsible for setting minimum technical requirements for interoperability and common operational security standards.

The CN, eIDAS Expert Group and eIDAS Technical Subgroup have working formats and meet regularly. There is also a good collaboration between the entities. For example, eIDAS Technical Subgroup provides detailed technical knowledge when needed, and the CN advises the eIDAS Expert Group in the legislative process. It is also important to mention that member state representatives in those three institutions often overlap. It means that an eID expert representing his/her country may participate in two or all of these institutions in parallel.

5.2.1 eIDAS Cooperation Network

The Cooperation Network (CN) is a formal network established under the European Commission implementing decision 2015/296 (implementing decision) to promote the cooperation between member states in the eIDAS regulation implementation [158]. The CN consists of representatives of the 27 EU member states[7] and representatives of the European Economic Area (Iceland, Liechtenstein and Norway). It is possible to include additional expertise to the CN on a need basis. The CN working format includes regular (approximately 3-4 times a year) online, on-site, or hybrid meetings and written correspondence. According to the implementing decision, the CN's main responsibilities are:[8]

- information exchange
- knowledge sharing
- peer review of eID schemes

Information exchange refers to the CN's responsibility to establish and maintain effective communication in eID assurance levels and interoperability-related matters (including technical issues) between the member state experts.
Knowledge sharing means that the CN members follow the latest developments in the eID field and exchange best practices. The aim is to share experience between the member states and ensure high security of eID schemes in the EU.
Peer review of eID schemes means going through the member state eID scheme under the notification according to the agreed procedure and providing an opinion on whether the eID scheme corresponds to the requested assurance level or not.

According to the implementing decision, the CN adopts eID interoperability-related opinions regarding eID schemes´ assurance levels defining minimum technical requirements, standards, and procedures. Furthermore, in its opinion, the CN sets also out the general regalement for the notification of eID schemes. However, it has to be noted that opinions in the European Union´s legal environment do not have a binding effect.

During its work, one of the main regulations that the CN follows is the EC implementing regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means [160]. This regulation

[6] https://ec.europa.eu/info/departments_en

[7] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

[8] Cooperation Network Resources. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Cooperation+Network+Resources

gives the CN experts a general framework for the assessment of eID schemes. A detailed overview of the assessment procedure and requirements is given in Chapter 6.

The CN working language is English, and working documents, peer-review materials, and outcomes are shared via e-mail and uploaded to the CN Wiki environment provided by the EC[9].

5.3 Notification of the eID schemes

eIDAS regulation article 9 describes the notification procedure. Fig 12 presents the eID scheme peer review process in practice. The peer review process usually starts from the pre-notification. It means that the notifying member state uploads the relevant documents to the Cooperation Network Wiki-based working environment before starting a peer review. During this period, all member states can have a preliminary look into the eID scheme and decide if they would like to participate in the peer review process. At the Cooperation Network (CN) meeting, the notifying member state presents the scheme, and member states can take the roles in the concrete peer review process. As the participation in the peer review process is voluntary, the actual peer review process will be carried out by the member states who have shown their interest in participating in the peer review process. In Fig 12, they are named as eID working group (WG) as they usually do not represent all CN countries. When the eID WG has finished the peer review, they present the peer review results, and most important findings, suggestions at the next CN meeting. Other member states can ask specifying questions, and finally, the CN forms an opinion about the eID scheme under the notification. The European Commission will publish the list of the notified eID schemes in the Official Journal of the European Union [42]. A more detailed description of the notification process will be given in Chapter 6.

Figure 12: eID scheme peer review process.

Currently, 21 countries out of the 27 member states have notified their eID schemes, and one eID scheme is peer-reviewed.

5.3.1 Overview of the Notified eID Schemes

In 2017, Germany was the first EU member state who notify their eID scheme on the level high under the eIDAS regulation, followed by Belgium, Croatia, Estonia, and Spain in 2018 [92]. Currently, 21 member states have notified their eID schemes. It means that six member states have still not notified (or not finalised the notification) their eID schemes. Bulgaria and Slovenia have recently just finished their peer review and eID scheme notification. Cyprus has expressed its will to pre-notify its eID scheme during the 2nd half of 2023. Moreover, many member states are willing to update their existing and already notified eID schemes.

Table 12 provides an overview of the notified eID schemes and eID means and their assurance levels. Some countries have not notified their eID schemes at the same time

[9] https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Cooperation+Network+Resources

but separately. However, in the table they are presented together.

Table 12: Overview of the notified eID schemes

Country	No of schemes	No of means	Level of assurance
Czech Republic	1	3	Low/Substantial/High
Estonia	6	6	High
France	1	0	Substantial
Italy	2	2	Low/Substantial/High
the Netherlands	2	3	Substantial/High
Sweden	1	3	Substantial/High
Denmark	1	6	Substantial
Spain	1	1	High
Malta	1	1	High
Latvia	1	4	Substantial/High
Germany	1	3	High
Slovakia	1	2	High
Croatia	1	1	High
Belgium	1	3	High
Austria	1	0	High
Luxembourg	1	1	High
Lithuania	1	1	High
Portugal	2	2	High
Liechtenstein	1	2	Substantial/High
Poland	1	2	Substantial/High
Norway	1	1	High
Total	**29**	**46**	-

19 schemes out of 21 are notified on the level of assurance (LoA) "high". Nine schemes are notified on the level of assurance "substantial" and only two eID schemes correspond to the LoA "low". That illustrates a clear direction to ensure a high security level of electronic identification in cross-border use cases.

Most of the notified eID mean under the scheme base on smart cards. However, some of the notified eID means under the scheme are mobile-based. A more detailed overview of the pre-notified and notified eID schemes under the eIDAS regulation can be found at the EC Wiki environment[10].

5.4 eIDAS Implementation in Practice

One of the eIDAS regulation aims is to enable mutual recognition of the notified eID schemes and encourage cross-border e-service provision and interoperability [42]. Two pre-conditions need to be met before the eID scheme can be used for the cross-border authentication [44]:

- the national eIDAS node of the country receiving the identification request needs to be in place and operational;

[10] https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

- e-service provider of the other country must be connected to the national eIDAS node.

Practical implementation of the mutually recognised eIDs is achieved via eIDAS nodes. A member state implements a node that is able to communicate with the nodes of the other member states to enable cross-border identification and authentication[11]. The eIDAS node acts two ways. It can request the data for the cross-border authentication or act as an authentication provider[12].

Fig 13 presents the high-level view of the eIDAS architecture. The eIDAS node contains three main components:

- eIDAS-Connector
- eIDAS-Proxy-Service
- eIDAS-Middleware-Service

eIDAS-Connector is used for cross-border authentication requests. The cross-border authentication service is provided using eIDAS-Service that can be integrated via eIDAS-Proxy-Service or using eIDAS-Middleware-Service[13]. eIDAS-Proxy-Service provides personal identification data in case the cross-border authentication request. eIDAS-Middleware-Service is an eIDAS-Service that runs Middleware provided by the member state, which sends the identification data and is operated by the member state who requests and provides the identification data. In case of using the eIDAS-Middleware-Service, it needs to be integrated with the eIDAS-Connector located in the member state requesting the authentication[14]. During the communication between the two eIDAS nodes, the national protocols of the communicating member states are translated into the eIDAS protocol[15].

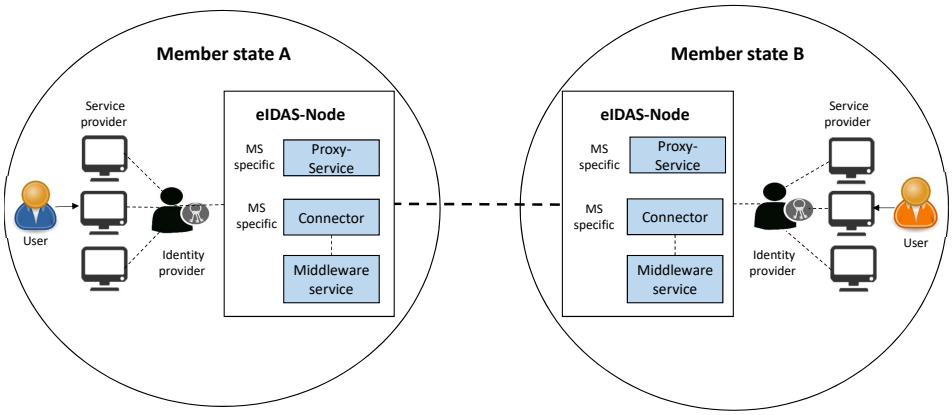

Figure 13: Main components of the eIDAS architecture. Source: CEF Digital home page.

After the implementation, the eID owners of one member state can prove their identity while accessing the e-services provided by other member states connected to the

[11] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/How+to+implement+or+operate+an+eIDAS-Node

[12] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

[13] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

[14] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

[15] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

node. Fig 14 illustrates the cross-border authentication process from the user perspective. If a person from a member state A would like to access an e-service provided by member state B, then during the authentication procedure, a member state A eID is detected, and the authentication request is sent to the member state A identity provider (IdP). When the user is identified, the result is returned to the member state B e-service provider, and access to the e-service is granted[16].

Figure 14: eIDAS cross-border authentication.

To make the eIDAS implementation easier for the member states, the EC provides sample implementation for the member states based on the technical specifications developed by the member states, the EC in cooperation with the eIDAS technical subgroup and the CN[17]. eIDAS node integration components are funded by the CEF (Connecting European Facilities) program. CEF is an EU funding instrument for EU-wide infrastructure projects, including digital initiatives[18].

According to the EC information from 29.07.2021, 24 countries[19] from 31, have implemented the eIDAS-Node and it is in production. The solution is under development in five countries (Cyprus, Greece, Hungary, Ireland, and Liechtenstein). In Romania, the development is planned, and in the case of France, information about the implementation status is unavailable. 25 countries[20] out of 31 reuse eID sample implementation software. Austria partially uses the eID sample implementation software. Five countries (Denmark, Germany, Hungary, Sweden, United Kingdom) have a specific eIDAS-Node implementation solution.

Before it is possible to use e-services across borders, the national eID scheme needs to be notified at the EU level. During the notification process, the member state eID scheme will be peer-reviewed by the CN members. Therefore, chapter 6 provides a detailed overview of the eID schemes peer review process.

[16] https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=82773030

[17] https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

[18] https://ec.europa.eu/info/funding-tenders/find-funding/eu-funding-programmes/connecting-europe-facility_en

[19] Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Iceland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

[20] Belgium, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Greece, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain.

6 Analysis of Existing e-ID Peer Review Routines in the EEA

The eID scheme peer-review process starts at the CN meeting. The notifying member state presents its eID scheme and invites the CN members to participate in the peer review process. Participation in the peer review process is voluntary. At the end of the CN meeting, the EC asks the member states to choose the roles in the peer review process. This Chapter provides a detailed overview of the electronic identity schemes assessment procedures, roles, and topics. Finally, the analysis of main regulations and guidelines used for the assessment is provided.

6.1 Roles and Responsibilities

The CN members can choose different roles in the peer review process. Every peer review has a coordinator responsible for the general coordination of the peer review and communication between the CN members participating in the peer review process and the European Commission. Usually, there is one coordinator, and according to the practice, the coordinator is not the notifying member state itself.

Based on the EC implementing regulation (EU) 2015/1502 [160], the peer review is divided into three topics: topic 1 "Enrolment", topic 2 "Electronic identification means management, authentication and interoperability", and topic 3 "Management and organisation". A detailed overview of the peer review topics is provided in sub-chapter 6.2. Every topic has a rapporteur, who is responsible for coordinating the discussions within the topic during the peer review process. Each topic has one rapporteur. However, sometimes one member state is a rapporteur in more than one topic.

The CN members can choose between two roles in the peer review process. They can participate as an active member or an observer. Fig 15 presents the roles in the peer review process.Participation in the peer review process is voluntary, and participation and taking roles are flexible. For example, the CN members can participate as active members or observers in one or all topics. They can also participate in different roles in different topics (e.g., they can be in the active member role in topic one and the observer role in topic two and topic three, etc.). The number of active members and observers in the peer review process is not limited. Table 13 provides an overview of the responsibilities of different roles.

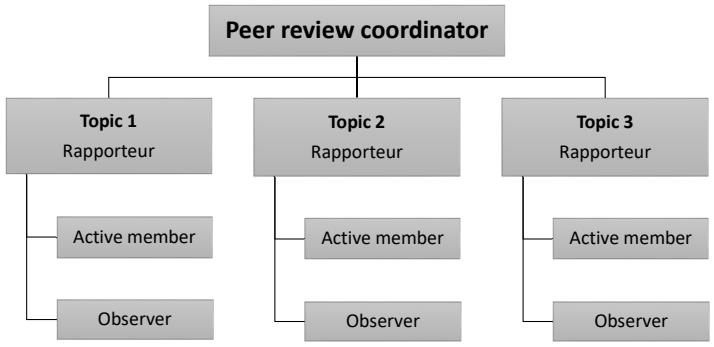

Figure 15: Peer review roles.

All these roles have different responsibilities in the peer review process. The coordinator plans the peer review process and The peer review coordinator is responsible for general planning of the peer review process. The coordinator prepares the peer review

Table 13: Responsibilities in the peer review process

Role	Responsibilities
Peer review coordinator	- Peer review time planning. - Information exchange management. - Time management. - Facilitator for discussions.
Rapporteur	- Responsible for chosen topic. - Raising concerns. - Drafting the topic for the report. - Keeping the deadlines.
Active member	- Active participation in the chosen topic. - Raising concerns. - Commenting the report. - Keeping the deadlines.
Observer	- Raising concerns. - Keeping the deadlines.

timetable together with the notifying country and coordinates the information flow between all the involved parties (including distributing documents, templates, etc.). The coordinator plans regular meetings between the involved parties and facilitates the discussions. However, the coordinator does not make decisions on behalf of the peer review group. The coordinator ensures that all agreed deadlines during the peer review will be met and is responsible for compiling the whole peer review report.

Each peer review has three rapporteurs, one for each topic. Rapporteur is responsible for a particular topic, driving active discussions and raising concerns as early as possible. As a result of the peer review, the rapporteur summarizes the most important findings of this particular topic in the peer review report and reviews feedback from the active members and observers. Rapporteurs can make decisions in the peer review process together with the members included in the concrete topic. They are also responsible for keeping the deadlines.

Active members ensure their active participation in the peer review process by asking questions during the question rounds, participating actively in the peer review meetings, and providing feedback to the peer review report. Active members should raise any concern they have with regard to the eID scheme under notification without delay. Active members participate in the decision-making within the topic. They also have to keep deadlines or notify the rapporteur and coordinator if it is impossible to meet the set deadlines for some reason.

The observer role is more inactive in the peer review process. However, they can raise concerns and ask questions if they have any. In addition, they can read and access the peer review documentation and keep themselves in the information circle. Observers must also follow agreed peer review deadlines if they want to contribute to the peer review. Initially, the role seems to have a supervisory role in the process. Still, in practice, the countries often use it to follow the peer review without additional obligations.

In addition to the already mentioned four roles, it is important to bring out the team of the notifying country. They are responsible for answering all the questions regarding the notified eID scheme. They also should participate actively in the peer review process and provide any further information or organise additional meetings needed for the eID scheme peer review. The notifying country should follow the agreed deadlines or inform

the rapporteur(s) and the coordinator if they require more time.

The role of the European Commission is to coordinate the overall peer review organisation and support the peer review team by offering meeting rooms, working environment, technical facilities, etc. They also monitor the peer review progress and help to solve problems encountered during the peer review.

6.2 Peer Review Procedure

Every eID peer review usually follows the same pattern of activities. Fig 16 presents the peer review steps. The peer review starts with a kick-off meeting followed by the first question round. At the kick-off meeting, the peer review coordinator introduces the peer review schedule and main routines. The schedule, participants, and details are described in the peer review agreement document.

In total, there are usually three question rounds. A question round contains two types of activities. First, the participating members can ask questions about the submitted documentation, and then the notifying country has time to prepare the answers. Questions are asked by topics. Before the third question round, there is usually a face-to-face or online meeting to clarify the open issues. The meeting duration varies from half a day to one and a half days, depending on the open topics. After the third question round, every rapporteur prepares input for the peer review report by summarizing the main findings of the peer review. The coordinator puts the whole peer review report draft together, and all participants have a chance to comment on the peer review draft in three rounds. Rapporteurs go through the comments and include them in the report or talk them through with the peer review participant who made the comment. In case of disagreement, the rapporteurs and the peer review coordinator try to find a suitable solution for all peer review participants. The final version of the report is sent to the Commission and presented at the next CN meeting.

Figure 16: eID scheme peer review detailed process.

In parallel with the peer review report, the coordinator and the rapporteurs prepare the CN opinion draft. After the CN has reached a consensus about the eID scheme under the notification, the opinion is adopted and published in the Official Journal of the European Union. After that, the member states have 12 months to recognise the eID scheme at the notified level.

6.3 Regulations and Guidelines

There are two types of documents followed during the peer review process. Firstly, obligatory documents like legal regulations,implementing regulations, and decisions, and secondly, documents that support the peer review process but they are not legally binding.

Legally binding documents, relevant in the peer review process are:

- eIDAS Regulation [42]
- Implementing Regulation (EU) 2015/1502 [160]

- Implementing Decision (EU) 2015/296 [158]
- Implementing Decision (EU) 2015/1984[159]

The eID peer review process is mainly based on the eIDAS regulation [42] and its implementation act [160]. Those acts together form a core documentation used in the peer review process to understand if the eID scheme corresponds to the requested level of assurance. Those legal acts are based on the technical specifications and standards provided by European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO), and the International Telecommunication Union (ITU). More specifically, the legal acts take into account the standard ISO/IEC 29115 that provides an entity authentication assurance framework and specifies four levels of assurance in the entity authentication [65]. However, the standard still needs to be fully incorporated into the legislation because, for example, identity proofing and verification requirements are different [160]. Legal acts also refer to the standard ISO/IEC 15408 that establishes the general concepts and principles of IT security evaluation and specifies the general evaluation method [64]. Regarding the information security and service management systems, the legal acts rely on ISO/IEC 27000 [67] and standards from the ISO/IEC 20000 series [66]. Implementing decision (EU) 2015/296 regulates and frames the CN work during the peer review and defines the CN´s responsibilities and outcomes. Implementation decision (EU) 2015/1984 describes the formats and procedures related to the notification of the eID schemes, including laying down the notification form template [159].

Other legally non-binding documents, relevant in the peer review process are:

- Opinions and decisions of the Cooperation Network
- Guidelines and other documents helping to ease the peer review process
- Standards

Besides the legal acts, the CN has a right to adopt opinions and decisions that form the peer review practice. As a result of the peer review, the CN publishes an opinion. The first opinion of the CN is from 2016. Opinions are not legally binding for the member states, but they reflect a consensus between member state experts in eID-related matters. For example, with opinion No. 1-2016, the CN adopts the first version of the eIDAS technical specifications [150]. As opinions contain valuable information about the peer review practice, it is important consider already adopted opinions while peer reviewing other eID schemes. This also ensures equal treatment of the notifying member states. From 2016 to 2022, the CN published 30 opinions. In addition, the CN has adopted one decision. In 2019, the CN adopted a decision on the need for open access to the NFC interface to support secure mobile use of electronic identity means [151].

In addition to the legal acts and the CN-adopted documents, several guidance documents help ease the peer review process and understand the provided legal documentation and forms. For the notifying country, there is a guidance for the application of the levels of assurance which support the eIDAS regulation [154]. An eID scheme notification template guidance was developed by Austria, Estonia, and the United Kingdom, available for the notifying country [14]. Regarding the peer review, some countries participating in the peer review process have developed and documented their own guidelines. For example, France and some other member states have created a document, "eIDAS Subgroup – Lessons learned from the concluded peer-review process". The document contains observations and ideas on how to improve the current peer review process. Unfortunately, the document is only for the CN´s internal use and is not publicly available.

Often the standards, already named in this sub-chapter, together with legal acts, are used in the peer review process to assess the level of assurance of the eID scheme. Fig 17 summarizes the relevant documents in the peer-review context. During the interviews with the CN experts, it became clear that in addition to the legally binding and non-binding documents, the practice of the CN member states also plays a vital role in the peer review process.

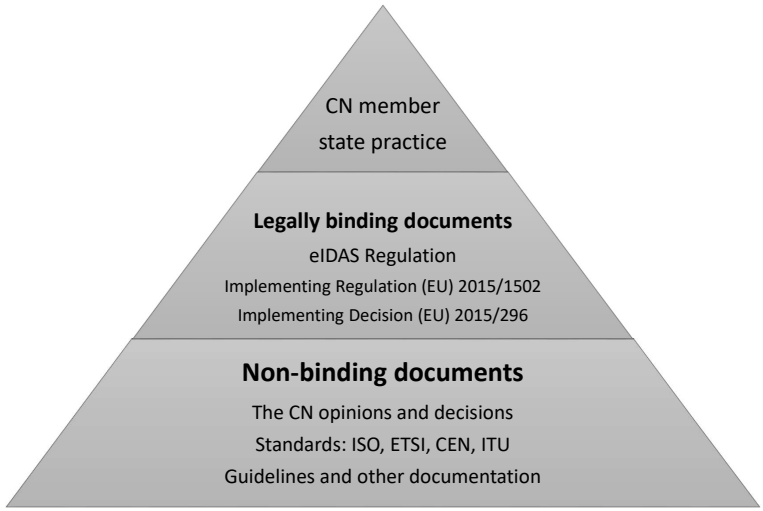

Figure 17: Relevant documentation in the peer review process.

However, the aim of the peer review is to ensure that the notified eID scheme corresponds to the requested assurance level in accordance with the legal regulations. Therefore, sub-chapters 6.3.1, 6.3.2 and 6.3.3 describe the main requirements for assurance levels "low", "substantial", and "high" by the topics.

6.3.1 Topic 1: Enrolment

According to the Implementing Regulation (EU) 2015/1502 [160], the enrolment topic comprises the following main subjects:

- application and registration
- identity proofing and verification of a legal and a natural person

It has to be possible to check that during the eID application process, the applicant is aware of the terms and conditions and recommended security precautions related to the use of the particular eID mean [160]. It is also important that the relevant identity data necessary for identity proofing and verification will be collected [160]. These requirements need to be fulfilled in case of any LoA.

Regarding identity proofing and verification, then there are different requirements depending on the LoA level. Also, there are differences in requirements applicable to natural and legal persons. According to the main basic requirements for the LoA "low", the natural person should have proof of an identity recognised by the EU member state where the eID application is made [160]. This refers to the valid identity documents that member states use inside the country to verify the people (e.g., ID cards, passports, driving licenses, etc.). All presented evidence for ID proofing needs to be trustworthy. It means that the

presented evidence is authentic and valid and/or from the authoritative source [160]. An authoritative source, in this case, can be any source capable of providing accurate information and data for identity proofing. It is also important that the claimed identity exists according to the authoritative source and that the person and the claimed identity are the same [160].

For the levels "substantial" and "high", additional requirements need to be met. For example, during the identity proofing procedure, the risks are mitigated by checking if the presented identity document is not lost, stolen, suspended, revoked, or expired. Moreover, in case of the LoA "high", the person has to be verified, for example, based on photo or other biometric identification evidence recognised by the member state. During the eID application process, the applicant needs to be identified through the comparison of the physical characteristics and authoritative sources. If the legal and natural identity is bound, it has to be possible to suspend and/or revoke a binding, and at the national level, there have to be procedures in place to manage this type of connection [160].

Detailed requirements for identity proofing and verification in the case of natural and legal persons are regulated in clauses 2.1.2 and 2.1.3 of the annex of the Implementing Regulation (EU) 2015/1502 [160].

6.3.2 Topic 2: eID Means

According to the Implementing Regulation (EU) 2015/1502 [160], the eID means topic comprises eID means management and authentication. More specifically following aspects are covered:

- electronic identification means characteristics and design
- issuance, delivery, and activation
- suspension, revocation, and reactivation
- renewal and replacement
- authentication mechanism

The eID means should utilize at least one authentication factor. For the substantial level, at least two authentication factors are required. It has to be guaranteed that the eID means is under its owner´s control. The highest level of assurance presumes additional protection mechanisms against duplication and tampering and protection against attackers with high attack potential [160].

The eID means should be delivered to the person to whom it belongs. Depending on LoA, there can be slight variations. It must be possible to suspend and/or revoke an eID means operatively. Reactivation of an eID means can be only possible if the conditions before the revocation are met. In case of renewal and replacement of an eID means, initial identity proofing requirements apply [160].

Regarding the authentication mechanism, it has to be possible to verify reliably the eID means and its validity. Furthermore, the personal data in the eID means should be stored in a secure manner. Security control mechanisms like guessing, eavesdropping, and manipulation of communication by an attacker shall be implemented [160]. Depending on a specific LoA level, the requirements vary.

Detailed requirements regarding the eID means are regulated in clauses 2.2 and 2.3 of the annex of the Implementing Regulation (EU) 2015/1502 [160].

6.3.3 Topic 3: Management and Organisation

Cross-border service provision presumes well-established information security management policies, routines, and risk management concepts. According to the Implementing Regulation (EU) 2015/1502 [160] the management and organisation topic comprises following subjects:

- published notices and user information
- information security management
- record keeping
- facilities and staff
- technical controls
- compliance and audit

The users must be informed about the applicable terms, conditions, fees, and possible limitations. Information policy shall enable informing the users about any changes related to the service. Users´ request handling process must be in place [160].

To control and handle information security risks, there has to be an information security management system in place. In addition, there is also a need for an effective record-management system ensuring lawful retention and management of data [160].

It is important that the staff and subcontractors related to the eID schemes are sufficiently trained and experienced. Facilities must be secure and protected against damages caused by environmental events. Unauthorized access should not be possible. Access to the information should be granted only need bases [160].

Technical controls include information confidentiality, integrity and availability protection, and protection against eavesdropping, manipulation, and replay. Cryptographyc material should not be stored in plain text, and all sensitive information must be transported and stored in a secure manner. Incident management needs to be in place [160].

The eID scheme needs to be audited periodically by an independent internal and/or external auditor, depending on the LoA.

Detailed requirements regarding the eID schemes management and organisation are stated in clause 2.4 of the annex of the Implementing Regulation (EU) 2015/1502 [160].

7 Input from Experts

In addition to the documentary sources, legal acts, and standards, analysing the existing peer review process from the experts´ practical perspective is important. This chapter provides an overview of how the member states assess other country´s eID schemes and answers to the third sub-question of this research: "How do the member states recognise eID schemes of other countries to enable the cross- border e-service provision?"

Real experience in the peer review process in different roles is important to reflect the actual peer review practice. Therefore, the author conducted ten qualitative semi-structured interviews with CN experts from nine different EU countries. The average experience in the eID field of the interviewed experts was 8.55 years. However, it has to be noted that two experts had more than 20 years of experience regarding the eID systems and their implementation.

The interview questions were initially divided into two parts and consisted of 20 questions. The first part focused on the peer review organisation, and the second part on the actual peer review process and working practices of the member states. Interviews were transcribed and analysed thematically using NVivo qualitative data analysis software. During the thematic analysis, the author first identified two main themes: peer review organisation and peer review of eID schemes. The first theme focuses on the peer review organisational aspects, like participation, environment, procedural steps, documentation, etc. The second theme already focuses on the peer review content and how experts identify that eID schemes correspond to the requested LoA level. The thematic analysis involves codes at up to four levels of detail. However, it is essential to point out that during the thematic analysis, it became clear that both parts of the interview contained information related to both main themes. Therefore, the presentation of interview questions did not follow the exact logic of identified codes and themes.

Detailed data analysis procedure is described in sub-chapter 2.3.3. The interviewees´ statements cited in this dissertation are based on transcriptions and are not edited. Therefore, used quotes may contain colloquial expressions.

7.1 Peer Review Organisation

The first part of the interview analyses peer review organisation, starting from the country´s decision to take part in the peer review process to the concrete working environment. Table 14 presents the ten questions about the peer review organisation. Questions were divided into three topics: participation decision (Q3-Q5), peer review process (Q6-Q9), and working environment (Q10). Based on the interview transcriptions analysis, it was possible to identify five main themes:

- participation
- process
- environment
- documentation
- harmonization

Fig 18 presents the overview of the main themes and related codes. The participation theme contains three codes: decision, topic, and roles. The author tried to understand on what basis the member states decide whether to take part in the peer review process and how they choose the topics and roles. Theme "Process" contains seven codes and

Table 14: Expert interview questions - Peer Review Organisation

Part I - Peer Review Organisation	
Question No	**Question**
Q.3.	Based on which criteria do you decide to take part in the peer-review process?
Q.4.	Based on which criteria are you choose your participation in different topics (enrolment topic 1, eID topic 2 or management and organisation topic 3)?
Q.5.	Based on which criteria are you choosing the role(s) (coordinator, rapporteur, active member and observer) in the peer-review process?
Q.6.	In your opinion, do you find the current peer-review process organisation (three question rounds, one face-to-face meeting, weekly meetings and three rounds of report review) sufficient to evaluate the eID scheme of a notifying Member State? Please explain your answer.
Q.6.1	Are there any excessive steps in the current peer-review process?
Q.6.2	Should there be any additional steps in the current peer-review process that enable better evaluation of an eID scheme?
Q.7.	Do you find the current pre-notification process useful?
Q.8.	What would be a sufficient timeframe for conducting the whole peer-review process?
Q.9.	What would be the optimal number of parallel ongoing peer-reviews?
Q.10.	Does the CEF working environment support well the eID scheme peer-review?

focuses on the peer review procedural aspects (pre-notification, time, expertise, meetings, number of participants, parallel peer reviews, disagreements solving) and experts´ involvement (their availability, interest, responsibility) in the peer review process. Theme "Environment" analyses the peer review group working environment and communication channels used during the peer review process. Documentation presented by the notifying country and its quality plays an important role in the peer review process. Therefore, the theme "Documentation" focuses on the eID schemes related documentation analysis. Finally, the theme "Harmonization" reflects the need for synchronization between the peer reviews.

7.1.1 Participation

This sub-chapter focuses on the theme of "participation" and presents the interviewees´ participation motivation in the peer review process. Participation in the eID schemes peer review process is voluntary. Therefore, the author wanted to know what motivates the CN members to take part in the peer reviews, how they decide their participation in topics, and how they choose the role.

When it comes to the participation decision, the interviewees´ named different factors. The author grouped the answers based on the common nominators and found that participation decisions are usually based on the co-operational and/or educational/informational grounds. Several informants named those aspects.

One of the core aims of the CN is to encourage collaboration between the EEA countries and build mutual trust. From the cooperation perspective, the interviewees brought out the following aspects:

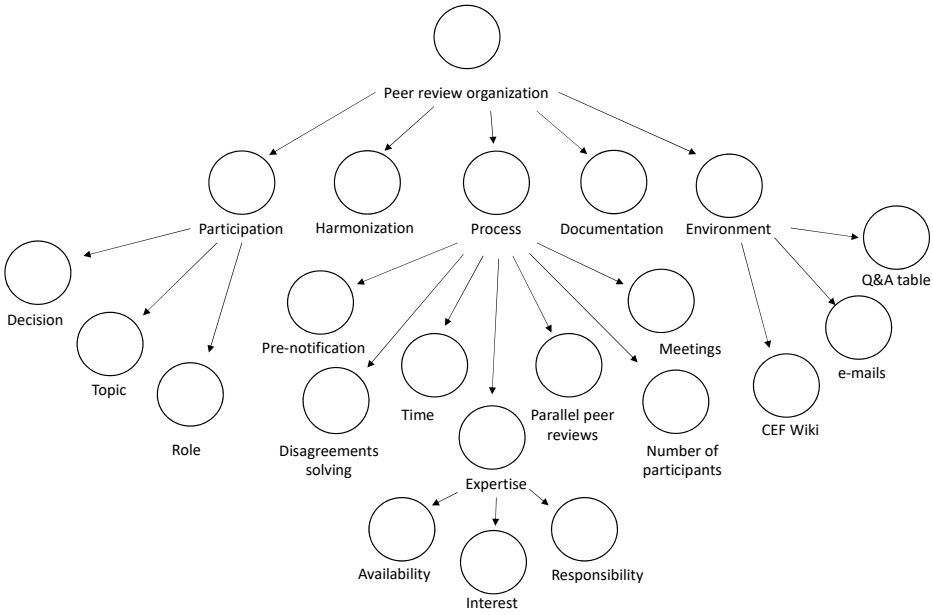

Figure 18: Theme "Peer review organisation".

> *"The selection has been mainly based on a region and partnerships. If we recognise that a member state comes to notify their eID scheme which is a very strategic partner for [name of a country], then we try to get ourselves involved in the peer-review process and get at least an observer role. And other countries that we do not have that strong partnership or any special interest to collaborate with them on more topics closely or specifically on an ID, we have been not very involved. "*

> *"If I may, the first one is reciprocity, because of some countries have helped us to notify our system and our means, that is point one. "*

> *"But it's also sometimes based on sort of some diplomacy where. Well, we take part in one peer review and they help us in ours for example. "*

> *"And it was also another good way to, I would say, try to participate in the projects of other member state and make so that we reach a common understanding. "*

However, one interviewee expressed disappointment that despite active participation in other countries´ peer reviews, the interest in taking part in the peer review of this particular country´s eID scheme remained low.

Knowledge sharing is another goal of the CN. Several interviewees brought out the possibility of learning something new from the peer review process about the other country´s practice or technology. In some cases, the aim was just to be informed and aware of what other countries were doing.

> *"One criteria first was interested in learning the system. So, as soon as we get a pre-notification, we can take a quick look and if there is some interest in the technology to learn something, then that is one criterion. "*

"And we see peer reviews as both a way to learn ourselves, because you must know that we are like late in [name of a country]. So it was a good way to learn first thing. "

"For two reasons to learn more from the other member states, and also to see if the eID schemes comply with the regulation, of course. "

"So I would say the main criteria to participate in a peer review for us would be first is it a new technology or not. Typically, we are less interested in peer reviews about smart cards, eID cards, wherever our protection profile certifications etc. are things that can be quite solid. And we are more interested about mobile application and video identification etc. "

"It is quite important to know what will be notified and have a say on the process. "

Some countries try to participate in as many peer reviews as possible. However, it is difficult as the same experts are often related to several eID-related initiatives, working groups, and projects. "

"We try to take part in as many peer reviews as possible, especially when we see that there might be some things which are an issue for us in the mainly in the registration process and the enrolment. "

"We try to follow each peer review, actually, because it's always interesting to have a look at the way it works on the other side. "

Some reasons for participation were mentioned only once. For example, a member state may decide their participation based on a possible significant discussion related to the scheme. Sometimes member states also participate to gain visibility, or because otherwise, there will be too few participants in the peer review process.

In some member states, the CN representatives are public sector officials, but some countries have delegated the role to a private sector service provider. In those cases, the CN representative consults with the public sector authority responsible for the eID schemes before taking the participation decision.

In addition to the participation decision, the CN members need to decide on what topic or topics they want to be involved in the peer review process. The CN members can choose between three topics: "Enrolment", "eID Means" and "Management and Organization". Table 15 summarizes the interviewees´ preferences to participate in topics. The preferences are brought out anonymously and cannot be connected to a particular CN member because the decision between the topics is a free choice of a country. It has to be noted that table 15 presents the general interest of the interviewees and does not mean that they could not be interested in other topics in particular peer review. However, it is visible that topic 1 and topic 2 are more interesting for the CN members. One interviewee even brought out separately that topic 3 is a bit boring.

The reason why the CN members prefer one topic to another varies. Some interviewees decide based on their personal experience and professional background, others based on the eID scheme and its technical solution under the peer review. At least two interviewees mentioned that as the peer review process is time-consuming, they try to make an optimal participation decision. However, some CN members prefer topic 3, because there are not many participants, and usually, there are much less disagreements.

Finally, the CN members have to decide their role in the peer review process. It is possible to coordinate the peer review, become a rapporteur or participate as an active

Table 15: Deciding between the topics

No	1	2	3	4	5	6	7	8	9	10
Topic 1	X			X	X	X	X	X	X	X
Topic 2	X	X	X		X	X	X	X		
Topic 3								X		X

member or observer. A detailed description of the peer review roles is described in subchapter 6.1. Table 16 gives an overview of the roles and interviewees´ preferences. Deciding the role is kept anonymous for the same reason as deciding the topic. The interviewees prefer to take active roles in the peer review process. Active in this context does not mean only the active role but also the coordinator and rapporteur role, as they actively contribute to the peer review process. Motivation to take an active role varies among the CN members. Two interviewees said they take rapporteur or coordinator roles to keep the peer review process functional and running.

> *"One of our reasons is that usually a lot of peer reviews going at the same time, and so if we want the mechanism to keep being functional, we have to participate as a rapporteur or coordinator sometimes. "*

> *"And in terms of involving myself as rapporteur pretty often, it is well, it is not that much additional work and it helps out when there is lack of other member states taking that role. Yeah, I mean, to keep the endeavour running. "*

Table 16: Deciding the role

Role	1	2	3	4	5	6	7	8	9	10
Coordinator		X		X	X				X	
Rapporteur		X	X		X		X	X		
Active member						X		X	X	X
Observer	X									

Sometimes, deciding the role can also be political or related to the technology under peer review. One interviewee pointed out that being a rapporteur gives a possibility to have more influence in the peer review process.

> *"If we see something really critical in the end, what the country has submitted, when we think okay, this is this critical, we wouldn't allow this form for LoA high for example, then we try to be the rapporteur to have more power, to take some influence on this issue. "*

The observer role seems to be least preferred. One interviewee even pointed out that he does not understand the necessity of the observer role.

> *"I've never really understood the observer role. Because the observer, what does it mean? The have access to the document, but you're not supposed to make any comment or to ask question. "*

The other interviewee added that the observer role is not used as it was initially planned.

"...because we have a role of observer in the peer reviews, which in theory should be used to just check if the peer review is going as it should. And it's not really used in practice, which is a bit sad, I would say. "

However, the observer role allows the CN members to keep an eye on the eID schemes under the notification when there is a lack of experts or time to take any active roles.

"...we had very few people who had a chance to put their time on participating in the peer reviews. So we kept it quite simple, tried just to be on picture or in the information field and at least get a notifications or documentation about the process. So maximum commitment was or has been so far been the observer as far as I know. "

7.1.2 Process

This sub-chapter covers the theme "Process" and attributes related to it. Fig 19 presents the codes of this theme. Theme "Process" comprises all components related to the peer review procedure, starting from the pre-notification of an eID scheme to the peer review resources like time and participants´ availability.

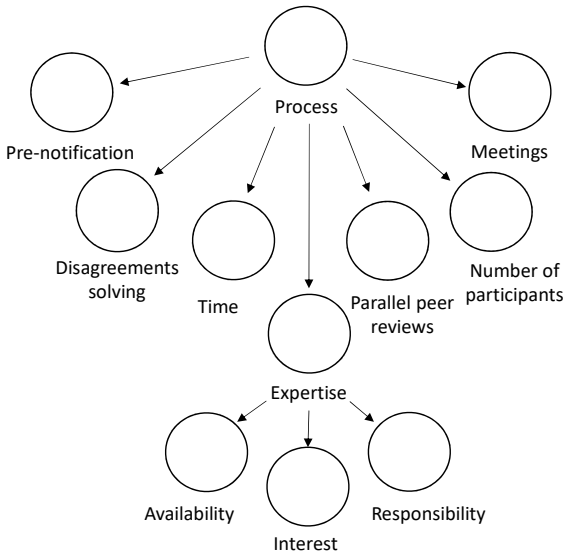

Figure 19: Theme "Process".

Peer review participants and their expertise determine the quality of the peer review. Therefore, expertise is one essential component of a peer review process. The interviewees brought out that one of the challenges in the peer review process is the availability of experts. If the experts are overloaded, they cannot focus on the peer-review documentation and the quality of work, and in the end trustworthiness of the final decision will be affected. Two interviewees said:

"But, it depends also on the availability of the experts from each country, how deeply they can dig in to the documentation and how much resources they have to focus on that specifically. "

"We have been lacking the personnel resources for participating in all the European peer-reviews previously. "

The other expert added:

> *"we have seen peer reviews where people are so full of other work that the participation is very minimal. And also sort of the engagement into it actually, look at all the things and keep up the I mean, it requires quite a lot of effort and resources to actually dig into all the details and sort them out. Which means that some countries are very closely looked at, and others more or less just pass through. That can be problematic from a trust point. "*

One of the experts admitted that due to the other responsibilities, it takes time to find time to go deep into the documentation.

> *"Now, of course, depending of the work we have beside this, we will, more or less deeply engaged in a peer review process, depending of our other constraint, especially and we'll probably come back on this later, when we talk about what works and what doesn't work. But especially today, since we were involved in the eIDAS expert group for the wallet, we are involved in consortium for the large scale pilot, everything beside or day to day work, I must confess, for instance, for the [name of a country] peer review, I couldn't take much time to deeply work on this. "*

However, some countries can still contribute and find enough experts who actively participate in the process.

> *"There is always a few countries that is a little bit more active than others, and have a lot of both experience and manpower to put into it. "*

In addition to the experts´ availability, the peer review process faces a lack of interest challenge. As there have already been around twenty peer reviews conducted, the process is no longer interesting, and the experts have started to lose interest. One of the interviewees summarized the issue as follows:

> *"They've done this process many times, so they're a bit like bored or they have other priorities sometimes. So at the beginning, there were way more questions, I think, during the question rounds. And now you see that there's less and less interest maybe to be involved. "*

Moreover, it is unclear what the actual responsibility and liability of an expert taking part in the peer review process are and how the expert´s technological preferences influence it. Peer review is not equal to the auditing procedure and does not certify an eID scheme. According to one interviewee:

> *"In, in particular, also related to what is the responsibility and, in fact, liability of the peer reviewers. Because in the current setup a peer reviewer, not claiming that has happened, but a peer reviewer that dislikes for certain reasons, technology a certain approach could simply insist on considering certain aspects of another scheme insufficient. And in what would be the result, when we have an opinion with some scepticism, which has a certain political impact on the one side. But the consequence for the peer reviewer compared to the consequence of an auditor that does produce a reproducible result that is really evidence based. There is a gap. "*

A bit broader topic from the experts is the optimal number of peer review participants. Currently, there is no lower or upper limit, as participation in the peer review process is voluntary. As a result, it is sometimes challenging to divide all the roles at the CN meeting. Especially when there is more than one peer review announced. Therefore, one interviewee suggested:

"Of course, suppose not so many country are able to participate in a peer review. That could that be a problem. So maybe we could find a way to improve the system requesting a minimum of peer-reviewing country for instance, so far, I've never noticed a problem due to a lack of participating member state, but it's the case it's probably not to be excluded in the future. "

That leads to another topic, which is parallel peer reviews. The author asked the interviewees about the optimal number of parallel peer reviews. Seven interviewees from ten found that two peer reviews in parallel are optimal, and three are already absolute maximum. Two respondents found that one peer review at the time would be the best, and one interviewee did not have an opinion about the optimal number.

Some interviewees found that the number also depends on the complexity of a particular eID scheme under the notification. For example, one interviewee pointed out:

"So, it depends on the number of authentication means on the eID means that are within one notification. So, in one pre-notification process, you can have more than one eID scheme. Depending on the documentation, two to three in parallel should be possible. But, if one of them is a large one, then it blocks time, of course. "

Interviewees also suggested how to make the peer review process smoother in case of parallel peer reviews. One interviewee suggested:

"I think we could also kind of fit one at the time on the schedule if there is a specific timeline. So, the Commission should make some kind of road map and queue for the countries who come to notify and give them a specific time slot for this. Of course, if the queue is very long, then there has to be some compromises because it does not make sense since you are ready to notify you eID, it is in production, and you cannot notify before a year. So, I guess one to two at the time is the limit. "

The other interviewee pointed out that a preliminary eID scheme audit would help save the expert´s time in the peer review process.

"What we're seeing here is that if we can have this external audit, a little bit better structured. So practice skills, practice practices declaration, in a more structured way, with how the audit criteria a little bit more clear, we do have a audit statement. If we can raise that, it would not be so resource consuming, and that you would have a better chance to actually participating in more. "

One interviewee found that all rapporteurs should be different in the same notification round.

"Also, it should be balanced in a way that the same rapporteurs would not be present for the all peer reviews. There should be a balanced participation where the rapporteurs should be different per each peer review. Because otherwise we will see all the three experts participating as rapporteurs in all peer reviews. "

Another interviewee proposed that to save time and ensure uniform coordination of the peer reviews, it would be reasonable to have one peer review coordinator for all peer reviews in the same round.

"It would be useful to have one coordinator for all three of the peer review. So the same coordinator. Okay. So then we, for example, plan the conference calls on the same day after each other, and then the coordinator can be a bit more like, practical instead of that you have three different coordinators who have to do the same things apart from each other. It could save time if it's the same person. "

The peer reviews are usually conducted between two CN meetings. The CN meetings are planned approximately every four months. The author asked the interviewees if this four-month period was sufficient for the whole procedure.

All interviewees found that, in general, the three-four month period is sufficient for the peer review. However, sometimes it also depends on the eID scheme under the notification, but the current period is mostly reasonable. One interviewee found that one week for questions is insufficient from the time planning perspective. He stated as follows:

> *"I think that to have only one week for collecting the questions and one week for answers, everything is in rush, it is very fast. By my opinion, it should be more time for that. "*

Some other interviewees found that if there were more time, people would still use the whole period, and there would not be any qualitative difference in terms of the final result. They reasoned their opinion:

> *"Because frankly said, if you have more time you will do all things longer and slower and definitely at the end of the process you will say that we did not have so much time. It is a human mind-set. "*

> *"I think the way it works today is not that bad. Having too long period, would not help probably because many times, the more time you have, the more time you take and not necessarily to do a greater job. "*

Two interviewees pointed out that the time to finalize the report is usually too short. One interviewee suggested that the report writing should be done parallel with the question rounds.

> *"I think the peer-review group should write the report as they go along, instead of having the three rounds, and then they start to doing the writing, it seems to be it's kind of inefficient, because then you could kind of incorporate all the knowledge you get from the questions into the report straightaway. And then you had a kind of a draft report for the face to face meeting, and you could have a look at that. "*

Regarding the peer review process steps, the author asked the interviewees about the necessity of the pre-notification procedure. Most interviewees found that having some information about the eID scheme available in advance is good. However, most of them admitted that they have time to look into the documentation when the peer review starts. One interviewee pointed out that the pre-notification process may be more beneficial for the EC. The interviewee reasoned as follows:

> *"...but maybe from a point of view of the Commission is necessary for them to check if there is something that is eligible for peer review and notification. And maybe they need the documentation before starting the request peer review process. "*

The other concern regarding the pre-notification is that the documentation is incomplete and may change before the peer review starts. Two interviewees described the situation in practice:

> *"We had it a couple of times that documentation was uploaded. I think [name of a country] for example in the last weeks did that. They uploaded a year ago something and now they uploaded new documents and said okay that are the relevant ones. "*

"Sometimes we have all the documentation need in other cases, we have a first iteration with some document published. And then before first meeting to the comments are updated, and then it can be also time consuming for the one who will review but otherwise, it doesn't work that bad in my in my opinion. "

The current pre-notification procedure is not fully described. Therefore, two interviewees mentioned that the procedure should be more structured and defined. The experts brought out the following aspects:

"I think the pre-notification is probably a reasonable, reasonably good practice. I think, if you would formalize it a little bit more, in terms of how you actually structure the documentation, how you sort of declare your practices, that would be beneficial, because it will be more comparable. "

"I think it's helpful to have this set of documents that everybody uploads, so they, you know, easily know where, where all the information is. So if everybody uploads, the same documents, then you know, okay, this document this introduction is the mapping. This is I think it's easier if there's like a guideline for this. "

But there are other topics. Where experts feel the need for additional procedures or guidelines, usually, the peer reviews go smoothly, and all questions will be solved during the process. However, in some cases, the participating countries are not able to come to an agreement regarding conformity to the eIDAS regulation and its implementing acts. Therefore, there is also a need for dispute-solving guidelines. One interviewee summarized the topic as follows:

"The second part is also that we do lack specific criteria or the guidance is something that is in dispute quite someone quite often, actually. So it means that within the group of peer reviewers, there is not always the same opinion on sort of what is required to achieve or fulfil certain control objectives in the in the regulation. "

One of the peer review process steps is a face-to-face meeting of the peer review group, where the notifying country gives an overview of their eID scheme, and experts can discuss open issues and ask additional questions on-site. The author wanted to know if the interviewees considered this practice useful. Three interviewees found the on-site meeting important because it is much easier to understand the other country´s system and gives a possibility for a country to demonstrate its solution. However, the concern is when exactly the meeting should occur, either at the beginning, at the end of the peer review, or somewhere in the middle. According to the current practice, the meeting is usually between the second and third question rounds. However, recent peer reviews have shown that if problems are raised before the final question round, it is challenging to finish the peer review report on time.

7.1.3 Environment

The environment in this context means different communication channels and an online environment that the experts use during the peer review. The communication channels include e-mail exchange and Excel table format used for the questions and answers, as well as the wiki-based online environment provided by the EC. The author wanted to know if the interviewees were satisfied with the existing communication channels.

Interviewees were used to e-mail communication. However, the Excel table format for questions and answers was not considered convenient from the usability side. For example, the interviewees bought out the following concerns:

"You cannot scroll properly. I hate this. But so, to answer your last question, first, I have no idea what could be another solution that might be better. But, the solutions are definitely not optimal. "

"So, I mean, even sort of the templates for the Excel sheets, and all that it differs from period from peer review to peer review and I don't even know where to find this template. So it's, that can be much more better structured, absolutely. "

One interviewee suggested that the questions could be visible for the notifying member state as they are placed, not sent all at once at the end of the round, and it would be possible to answer them as they appear.

"I think that could be done a lot smarter than Excel sheets. Kind of why not just put them in dynamically. And you could see the questions as they come along. Why do we have to wait for an Excel sheet that comes at a given point in time, it would be much better to actually have them kind of immediately when they are made. And then you could also answer them immediately. "

However, the interviewees did not propose any other concrete alternative solution for placing the questions and answers. Previously, the wiki-based online environment was used for that purpose, but it was not easy to use. According to one interviewee:

" There was a time in the past we have questions were submitted into the Corporation Network space. I remember that, it was the case in first peer reviews, but I think it was probably more difficult to use that, but just an Excel file where you can, you know, add new columns, comments, etc. "

Some interviewees admitted that they are not using the online environment and relying only on the information provided by the peer review coordinator by e-mail. Others find it a useful platform, but the functionalities are not used in the best possible way. One interviewee admitted:

"I mean, it's not a joy, actually, to log on to this conference space. I mean, everyone has been lost there. But it does work. I mean, it's at least a tool we can use. So I wouldn't say that this is a big problem for peer reviews. "

Two other interviewees added:

"I think it could be used in a more effective way, because it's very useful, useful platform. But now we don't use it enough. "

"I think the tool works fine for the document provided by the notifying member state. For the peer review itself, it really depends on the way it's managed by the coordinator, because sometimes documents are uploaded onto the environment, sometimes not. "

In light of the EU digital identity and the digital wallet, one interviewee found that the whole process, including the working environment, needs to be overlooked and re-designed.

To summarize this topic, the interviewees were more or less satisfied with the online environment and other communication channels. However, the wiki-based environment could be organised more efficiently, enabling better usability.

7.1.4 Documentation

Documentation in this context refers to the information the notifying country provides about its eID scheme. There is no list of documents that must be provided, and according to the current practice, the notifying country usually tries to follow the practice of the countries who previously notified their schemes, or they provide the documents they consider important from their perspective. Therefore, the author asked if the documentation provided by the notifying country is sufficient or if any important information needs to be included.

Some interviewees found that the sufficiency and quality of the documentation highly depend on the eID scheme and how it is described. Interviewees admitted that the quality of provided data varies. Interviewees explained as follows:

> *"That actually hardly, strongly depends on the data provided and the documentation and the quality of the documentation. We have seen different quality levels, I would say. So, what is important in my view is that the right documents are available and you can use them. "*

> *"I mean, it depends on the scheme and how it is described. I think there were some pretty good example where from the white paper you could learn the scheme and then with the LoA mapping where the LoA mapping case sufficient detail to address all the requirements, and I mean, at the end of the day, it is the law requirements that need to be addressed. "*

> *"It really depends on how well they are written. There are member states that have some good LoA mappings and some good White Papers and there are some that don't get quite sufficient information on the topic. "*

Interviewees considered White Paper and LoA mapping documents essential but insufficient. White Paper should give experts an overview of the eID scheme, and the LoA mapping document should focus on how concrete LoA requirements are fulfilled. One of the interviewees explained:

> *"Meaning a White Paper in order to give you an overview of what the system is because you see it mostly the first time in your life. And secondly, the LoA mapping in order to see how, which level of assurance is fulfilled. And in past times, it was not available in the beginning. "*

The other interviewee added:

> *"I think, potentially white paper and LoA document are sufficient. "*

Two other interviewees specified:

> *"My experience for basic information, the white paper and LoA mapping are useful, but when you want to go in details, other documents are necessary, because you cannot put everything in there in these ones. So I don't think these ones are just sufficient, you need a lot more usually to really understand. "*

> *"If the documents are properly structured, normally, they should cover all the aspects, at least for first assessment, in my opinion, and often LoA mapping and white paper do the job. "*

Interviewees made several proposals to improve the peer review documentation. One interviewee described the situation and proposed to re-structure the peer review template:

> *"Or maybe we could from the beginning, restructure of the peer review template, in order to at least mention all the possible sub-question regarding to notified schemes. Because today, I think everything that we use today was based on the first peer reviews from [name of a country]. And everyone adapt the document its own way, but we could probably find a way to for the future to wherever more elaborated template trying to cover all the different aspects, of course, it will never be fully satisfactory. But at least we could reach some kind of common baseline. "*

The other interviewee found that the documentation should be structured in a better way to make different schemes more comparable. Two interviewees reasoned:

> *"Definitely, it should be well structured for the notified schemes to be comparable somehow. So, I think it little bit lacks the standard of the structure to be easily compared with other attributes that the other member states publish in their specific documentation. "*

> *"But as I said, I think if we can have a little bit more structured practices document more of a template, it's like a big notification doesn't mean that there is this notification template. If you could have something look more like a CPS even though it's not PKI based here to actually show me on the topics you want and under it's a little bit more structured approach to it. "*

One interviewee brought out that the only required document is a notification form, which needs to be revised. The interviewee suggested that questions should be given in advance that all notifying countries should cover in their documentation. The interviewee reasoned:

> *"So I would say what you could fix would be a set of, let's say, 20 questions that need to be answered. And that should be answered in each case. "*

Often the scheme descriptions are long, and it is hard to get the overall picture. Therefore, one interviewee suggested including the general schema of the eID ecosystem in the documentation:

> *"I think what we got what we meant to make it mandatory to deliver some sort of overview of the scheme and the simple steps like in one shorts, controlled image. "*

Moreover, the same interviewee suggested:

> *"From the technical eIDAS node operator point of view we see that we need to have an overview whether they notified eID scheme can or cannot be consumed by the private sector e-service providers in another member state. That ´s one thing that has been lacking for sure. "*

Finally, according to one interviewee, there is a peer review lessons learned document prepared by the CN members, containing recommendations like standardizing some formats and listing a minimum set of mandatory documents. The interviewee explained:

> *"There was a document of lessons learned from a peer review that has been redacted by [Name of a person] last year, of the year before. And there was several recommendations. Like, for example, having a minimum set of mandatory documents to provide. Having a format for certain things. "*

Based on the interviews, the current documentation and template practice needs to be overlooked, especially from the structural point of view and the possibility of having minimal mandatory documents notifying countries need to provide.

7.1.5 Harmonization

During the peer review process, the experts should be able to understand if the eID scheme under the notification corresponds to the requested level of assurance (LoA) based on the eIDAS and its implementation acts[42, 160]. The country can notify their solution on the levels "low", "substantial" and/or "high". Within one notification can be several eID means that correspond to different LoA levels. Every eID scheme is differs from another, and experts need to ensure that eID schemes with the same LoA level are comparable. Ideally, it should be like this. However, there is a need for harmonization between the eID schemes and their assurance levels. One interviewee brought out:

> *"I think what we lack today is some means to ensure harmonization between the different peer reviews, because in the end, it's up to the coordinator and to the reporters to set the pace of the peer review. And we lack harmonization. "*

Therefore, the author asked the interviewees whether already notified eID schemes and their LoA levels were comparable. For example, if the member state A LoA "high" eID scheme and member state B LoA eID "high" scheme are equal when it comes to enrolment processes, eID means and management and organisation.

According to the interviewees, the notified eID schemes with the same LoA level are more or less comparable. However, some interviewees admitted that there are differences between the countries and schemes. For example, one interviewee reasoned as follows:

> *"There are differences; I think there are always schemes that have undergone the peer review process. And whether it has been an opinion of a Cooperation Network stating that it is level "high" indeed. Now, when you look at them, there are differences in terms of security of the components that are used. And this is a fact there are levels of certifications, there are very different levels of certifications that are used in the continental schemes, which are not fit to protect against the same type of attack. So this is what we have today. But where all of level "high". "*

Two other interviewees added:

> *"Kind of, but there are differences. There are differences that are hard to argue and also depend on the willingness of the notifying member state to get into a commitment. "*

> *"I think, they cannot be comparable. Every scheme is something special, something specific. Every country has the old scheme, specific scheme. How can you compare it? One member state has the general register of everything, the second does not have it but it is supplied by more databases or registers etc. We cannot compare it. Because of every country has own solution, and that is the problem. "*

One interviewee brought out that during the peer review, the experts take into account the specifics of a notifying country. The interviewee said:

> *"So it has shifted in this context, the assessment a bit, always taking into account the special circumstances of every member state and especially systems but it has definitely shifted. "*

According to one interviewee, the eID schemes with the same LoA level cannot be comparable. The interviewee explained:

> *"And also, if you start comparing the resistance against high attack potential discussions we have on some mobile systems, which have sandbox and secure element and so forth, compared with smart card systems, where the keyboard and the PC are the weakest links and ignored. But the same discussions apply to the mobile, I think we compare apple and oranges. "*

One interviewee pointed out that eID schemes that were notified in the beginning, when the peer reviews started, are not comparable with those currently under notification. The interviewee explained:

> *"I would say all not for several reason. Because, of course we started some years ago with the first peer review from zero and step by step we try to find a common understanding of what should be done for which LoA and it's clearly not a rocket science. And as we mentioned in the beginning, depending of the concurrent peer review that we have to deal with at certain moment, we can spend more or less time on it probably it also influence the final result. So no, all notified schemes, since they are different, are not fully comparable for SM LoA. "*

The reason behind it is that the peer review participants have learned during the process and started to notice new important criteria. For example, one interviewee brought out:

> *"Yes, recently one colleague from the Ministry of Interior highlighted that there is actually no biometrical data expiration date set in the levels of assurance requirements for example for LoA high. And how do you compare with this. You can only dig into the each of everyone of this notifying schemes documentation and there is no clear topic or attribute where you can actually see where it comes out because you have to read it between the sentences. And sometimes if you are not really looking for it, you will not see it. And you will see it afterwards when the peer review is done and then you discover that this eID scheme that has been notified few years ago actually should not have LoA high. "*

Another good example is lost and stolen checks of identity documents. This aspect was not brought up in earlier peer reviews. The interviewee explained:

> *"Because sometimes in the beginning, maybe now we have peer review, we have the loss and stolen check loss and stolen check with maybe some peer reviews before that question was not raised or not asked them. Yeah, if the concern is not raised, and it's not included in the recommendations or the in opinion. So it's still like, you don't know 100% if it really complies. "*

In this case, those countries just notified their eID scheme without meeting these particular criteria. The same interviewee continues:

> *"Yes, they got away. Maybe they don't have lost and stolen check either. But yeah, it's already approved. "*

A similar example was given by an interviewee using biometric remote identification as an example. The interviewee found that, in some cases, the peer review was easier for countries that went through the process earlier. The interviewee explained:

"And it has, I mean, this discussion about sort of biometric remote identification. It has evolved. It's something that has been I mean, the questions are more mature now. So it means that someone who did this earlier on was probably off easier. "

Finally, one interviewee admitted that the peer review standards have lowered over time:

"So we have somehow in the last years lowered the bar in order to fulfil and options high for example, regarding the secure element usage, on the first glance, it was excluded. All devices without secure elements. "

One interviewee suggested improving the process and making the same LoA level eID schemes more comparable. The interviewee proposed:

"If we want to compare them and we have a regulation that obliges each and every country to follow certain structure and format and requirements. Then, I guess there is no other option than to have at least a light peer review per each of this scheme that has been previously notified to provide extra information and to be reviewed by the peer-review organisation. "

Based on the interviewees' feedback, the eID schemes and their LoA levels are not fully comparable, and several components need improvement. Those countries who notified their schemes earlier had an advantage in terms of questions and requirements. However, it is clear that during the peer review process, it is important to consider a country's particular solution.

7.2 Peer Review of the eID Schemes

This chapter focuses on the peer review process and how experts review eID schemes. The author tries to understand the internal work process of the peer review participants, what documents and standards they take into account while peer reviewing the eID scheme, what are the most difficult parts of an eID scheme to assess, and how different social and cultural aspects affect the peer review process. Table 17 presents the twelve questions about the eID schemes peer review process.

During the thematic analysis, the author identified that the theme "Peer review of eID schemes" contains three main sub-themes: "Assurance levels", "Peer review routines", and "Factors influencing peer review". Fig 20 gives a detailed overview of the themes and codes related to the eID schemes peer review. Theme "Assurance levels" presents the experts´ understanding of assurance levels "high", "substantial" and "low". Theme "Peer review routines" includes codes related to the expert´s working process, how they peer review the eID scheme, what are the most important parts for them, what kind of documents and materials they use during the peer review process, what parts are the most complex to assess, etc. The third theme, "Factors influencing peer review", gives an overview of different personal, social, cultural, and historical factors influencing the peer review process.

7.2.1 Peer Review Routines

Every country has its way of working with peer review documentation. This chapter gives an overview of how the countries peer review the eID scheme, the most important parts that always need to be checked, what documents they take into account, and what parts of the eID scheme are the most challenging to assess.

Table 17: Expert interview questions - eID Schemes Evaluation

Part II - eID Schemes Evaluation	
Question No	**Question**
Q.11.	Do you find the documentation that the notifying member states is required to present (White Paper, LoA Mapping etc.) sufficient
Q.11.1	What kind of documentation or information is often missing for you?
Q.12.	Please describe your work process when you start evaluating the eID scheme. How do you start the peer-review process?
Q.12.1	Do you engage other people and/or authorities in the evaluation process? If yes, who?
Q.13.	Which documentation/legislation/standards do you take into account while peer-reviewing the eID scheme?
Q.14.	What are the main components (key points) that you always check while reviewing the eID scheme?
Q.15.	In your opinion, what are the main differences between the eID LoA "High" scheme and the eID LoA "Substantial" scheme?
Q.16.	What are the components of the eID scheme that you find the most complex to assess?
Q.17.	Considering the eID schemes that have been notified so far: do you find that eID schemes with same LoA level are comparable?
Q.18.	Do you think that LoA "Low" eID schemes should be notified on the EU level?
Q.19.	In your opinion, how much do different social and cultural aspects affect the eID peer-review process?
Q.20.	Is there anything else you would like to add?

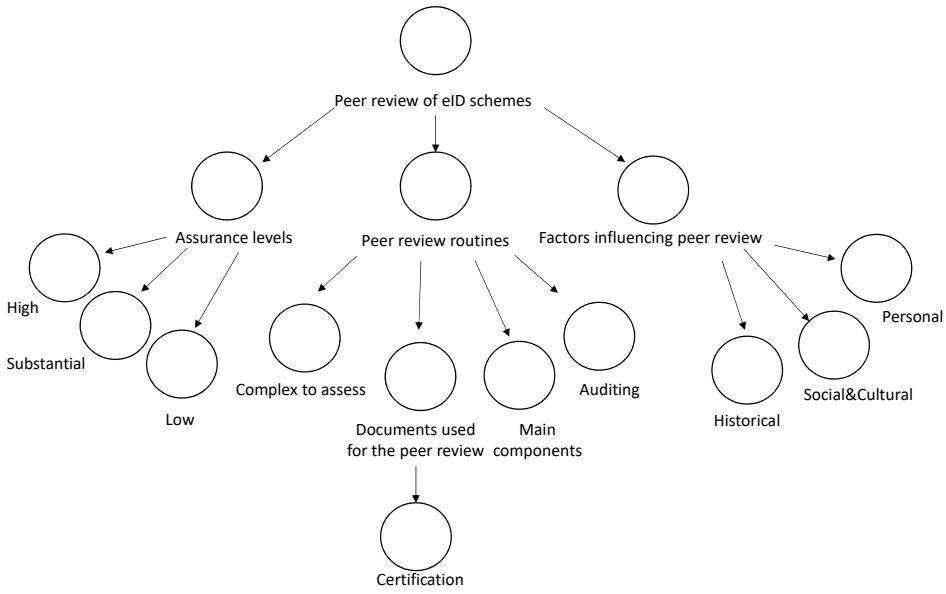

Figure 20: Theme "Peer review of eID schemes".

Six interviewees out of ten mentioned that they usually go through the peer review documentation and formulate the questions alone. Others said they have a small team (2-3 people) dealing with the peer reviews. In some member states, private sector representatives perform the CN expert role. One member state uses advisory cooperation during the peer review if needed. The interviewee explained:

> *"We have an advisory cooperation that we send the questions to the documents to, and they send us some questions that we can ask the member states and we for ourselves, we usually start with a white paper and all the other documents and then we stop by the enrolment and look okay. But what is there? Are there any things, which are unclear? How's the process and try to come to some questions. "*

One interviewee specified that in the case of several parallel peer reviews, one expert is responsible for each particular peer review. The expert reasoned:

> *"Otherwise, normally, for instance, if we were working concurrently on several peer reviews, one person will work on one peer review, and we will maybe discuss besides this, but most of the time, okay, review is covered one by one expert from organization."*

Mostly, the experts start the peer review by reading the LoA document, notification form, and/or the White Paper and try to get the first impression of the eID scheme. In case of specific technical questions, the other experts may be engaged. One interviewee explained:

> *"no, most of most of the time when experts do the peer review on our site, except if we have a specific question regarding a technical point, for instance, or specific algorithm mentioned for which we have some question, then we may address the question to some of our technical teams. "*

Based on the documentation, they form the first set of questions. One of the interviewees summarized the working process as follows:

> *"I do that all on my own. I'm not involving anybody else. Because I can do everything on my own. I have all the competence in all the fields. So that's quite easy. So I basically read the documentation. And once I've read the documentation, I'm noting where I think there are questions, and then I asked the questions, and that's essentially it. "*

7.2.1.1 Peer Review Main Components According to the interviewees, the peer review process is time-consuming and requires familiarizing with an extensive amount of material. Therefore, the author wanted to know the essence of peer review and what components in the eID scheme are the most relevant ones. To explain the question more, the author asked interviewees to imagine if they had twenty minutes to check the eID scheme documentation, then what would be the most important parts they would definitely check. One interviewee explained that the way, the expert approaches, depends on the requested LoA:

> *"I think the main questions, which are a bit the same, when we decide to participate is it a level "high" or level "substantial". If it is level "high", it raises more flags. "*

Fig 21 summarizes in a matrix diagram format the main peer review components brought out by interviewees. Based on the interviewee´s feedback, it was possible to divide the components into four main categories:

- enrollment
- authentication factors
- interoperability
- security

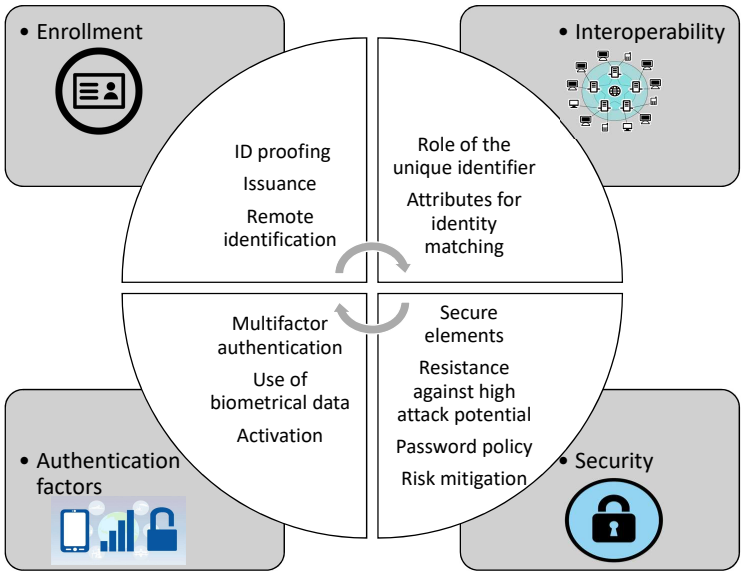

Figure 21: Peer review main components.

Enrollment is one of the core topics of the peer review. The interviewees found it important to check the identity proofing and issuance processes. Especially when it comes to remote identification and its correspondence to the LoA requirements. Three of the interviewees emphasized the following:

> *"The type of identification related to the level of assurance, so video identification versus face to face related to the level of assurance, that is one key point. Second key point is related to the issuance in principle, so just to get an idea, the activation issues and the most important point when we look at the authentication mechanism, so usage in principle. "*

> *"And most importantly, is the enrolment process. "*

> *"For the enrolment, here, it has to be made sure that you can be sure 100% that the owner of the ID has really gotten eID and no other person is able to get this his ID of course key confidence. And most importantly, is the enrolment process. "*

Other interviewee stated:

> *"Certainly the ID proofing phase. So certainly the activation and issuance processes. "*

In addition to the enrollment processes, the interviewees consider authentication factors important. One interviewee explained:

"Well, definitely I will see which is the enrolment process and which are the authentication factors they are using, which is their structure. How much they are using biometrical data on the authentication. "

The other interviewee added:

"Well has to be multi-factor authentication, of course. "

Interoperability is one topic that interviewees separately mentioned. However, it is not a separate part of the peer review documentation, and experts need to make conclusions based on the three topics covered by the peer review. Interoperability contains the concept of a unique identifier in the scheme and attributes used for identity matching. One interviewee explained:

"Actually, not on the level of assurance, but that is more really on the interoperability part. And that are questions that I had almost in any peer review. The focus of the documentation was mainly on the security aspects but the role of the unique and persistent identifier where the private sector parties are integrated, which attributes can I get for identity matching, in particular if there is no persistent identifier, those are the aspects that I always want to see. The rest is more reading the white paper, drawing a picture in terms of understanding the system. "

Moreover, the same expert brought out that often, the notifying countries describe mostly national aspects related to the eID scheme. However, the peer review is to identify the suitability of the scheme for cross-border use cases.

The other expert shared the view that there is a lack of interoperability information in the peer review process and explained as follows:

"I think this interoperability should have more focus on. Especially, for the eIDAS node operators, where can we get the information how they have enabled the eIDAS nodes or how they are using cross border infrastructure to provide the eID for other member states. Afterwards they will be notified. May be that will help a little bit, because I think there is a lack of description on the technical side of the cross border infrastructure implementation and I am here talking about eIDAS nodes software where many member states use the Commission provided reference implementation also in production because they do not want to change anything in the code. There are countries who are also operating their own code or version of the eIDAS nodes. That would be very interesting for me exactly to know ahead how they will be connecting technically to our ecosystem. "

Several interviewees mentioned security aspects. Therefore, it was considered a fourth important component while peer reviewing the eID scheme. However, security is a broad topic, and it is possible to approach it from different angles, from the technology components and their security to the risk management activities and password policy. Risks are often considered to be higher in remote identification cases. One interviewee stated:

"For me, password policy and remote identification, so I just check the basics, and basic security and secure elements. "

The same interviewee continued:

"For a substantial is it remote identification or not. Is it totally automatic or not. If it is level "high", is it just a mobile application. Or is there a smart card or secure element or something. So mobile application will be we will need some kind of proof that it is indeed fit for level "high". "

The other interviewee said that their country checks if the notified solution is resistant against high attack potential and whether the security risks are properly mitigated:

> *"So he always checks those components in documentation, if it's resistant against attack potential high or if how they mitigate those risks, and he always looks at those components. "*

From the challenges perspective, one interviewee pointed out that having standardized procedures and checkpoints is not always good because it makes adopting new technologies much more complex. The interviewee reasoned:

> *"But I think that's a problem. Because if you have these basic check marks, then you get into this static kind of situation. And then it's really hard to come up with a new scheme that breaks the existing normal rules. I mean, right now, the normal rules is that you have to show up physically, if you want to register at level high, normal rule is that you have to have certification, the best is your routine, certification etc. And I think to all those normal rules are kind of a little bit dangerous, right? Because this is a very dynamic world. And we are always to new ways to do things, new ways to identify people, new ways to authenticate, etc. And because it's kind of put into this little bit static framework that the review processes is, and people have their opinions, this is how it should be. "*

Therefore, it is also essential to see the eID scheme as a whole and unique, not only focusing on specific components and their compliance with the particular assurance level.

7.2.1.2 Assessment Challenges In addition to the main components, the author wanted to know what parts of the eID scheme are the most complex to peer review. From the comparative point of view, it is important to understand the unique parts of the scheme and treat them accordingly. It does not mean that unique parts should be automatically excluded from the peer review scope. However, it rather helps to prevent disagreements between the peer review participants and enables common recognition among the experts that particular parts of the scheme do not have to be always comparable with other schemes.

Based on the interviews, it was possible to notice three main topics that experts found a bit more complex to assess. These were: interoperability, security, and use of technology. However, it has to be noted that those three topics are often related (e.g., technology and security), and the presentation given by the author is just one possible way to present the interview results in a more organized way. Fig 22 provides an overview of the topics brought out by the interviewees.

The interoperability topic was not described in detail, as this part was generally considered missing from the current peer review. Therefore, the author just brought out the technical implementation of the eIDAS Node solution. In addition to the technical implementation description, one of the interviewees brought out the private sector aspect of the eID scheme. The interviewee explained:

> *"I think this private sector enable and may be describe whether their eID scheme will be, whether the transactions used for the electronic identification with notified means will have any financial. Will you have an obligation to pay for the transactions as a country or what are the options for accepting the eID on the private sector side. Whether there are any special requirements for providing the eID scheme for the private sector service providers in other country. "*

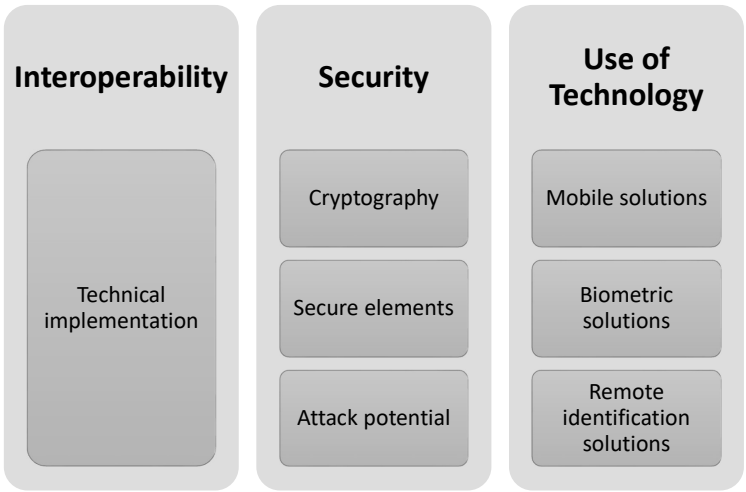

Figure 22: Peer review components that are complex to assess.

Security and its different aspects were the other main concern. Here, the interviewees found evaluating cryptography and secure elements in eID schemes difficult. Two interviewees said:

> *"I think that security. Security is, from my perspective, should be. It ´s often critical, it must be very complex and from my opinion, it is complex in the peer review. "*

> *"I would say the most complicated would be assessing cryptography and security of secure elements and like that. "*

The same interviewee continued:

> *"I think the majority of the members of the Cooperation Network are not cryptography experts, the security of components, but it is easy as long as we have certification reports or things like that. "*

Moreover, it is challenging to evaluate security risks and vulnerabilities. Especially when it comes to giving an opinion about the attack potential. One interviewee explained:

> *"Complex is to assess whether there are ways for an attacker to act like a man in the middle or you have it would be possible to steal things and act like the person. This is sometimes really complex. Are there any vulnerabilities in the system. "*

The author summarized the last part under the use of technology or, in other words, technology assessment. The interviewees approached the topic from a technology perspective but also how particular technology is used in the scheme. At least two interviewees mentioned complexities related to mobile-based technologies. They gave the following explanations:

> *"In terms or assessing, for me the most complex part is with the mobile eIDs and in particular, when the compromise any member state has between a perfect world of no vulnerabilities vs what the citizens have. "*

> *"The device I would say. With mobile solution, the overall solution really is very often device dependent. If you use the last iPhone or a basic smartphone, it will not be the same and ideally, we should have some kind of white listing of all kinds of device because the overall solution will really depend of the way both software and hardware components are working. "*

It also depends on how the concrete technological solution is used in the system. For example, in the case of biometric solutions, the technical part can be certified and quite clear. However, when the solution is used in the remote identification process with other technologies, it is difficult to form an opinion about the assurance level. Two interviewees reasoned:

> *"If you consider for instance, the use of biometric, biometric is fine, but of course, it depends if you combine it with a secure element or node or Trusted Execution Environment will depend on the algorithm using microfiche on the device. "*

> *"And the biometric functions are very, very, very hard to actually evaluate and there are, the significance is so big, it's actually a lot of risk going in there. And we can't really evaluate it. That's the headache. "*

The other interviewee explained the complexity in the case of video identification as follows:

> *"I mean, obviously, it's this specifically unattended remote video identification, that is the cause of a lot of discussions currently. And it is a black box more or less. And even when you see some test reports, if you would look at sort of the attack potential that they are evaluating these functions against, it's something around moderate or low, it's definitely not a high. "*

Another interviewee added:

> *"Video identification starts to be a bit tricky. And we do not have a real certification scheme, harmonized certification scheme for that. It's still something but at least we can pretend to understand with identification smart cards, cryptography, things like that. "*

If it comes to suggestions, one possible way to overcome these complexities is to include certification at a certain level in the peer review process. The interviewees did not have concrete certification proposals, but some interviewees mentioned the importance of certification during the interview. For example, one of the interviewees found that eIDAS and its guidance are weak and suggested to follow, for example, National Institute of Standards and Technology (NIST) documentation. The interviewee stated:

> *"So it is the eIDAS regulation is too weak, the guidance is too weak while the American NIST standard that is really strong, it is operational. "*

That is also one reason why the author separately analyses the documentation that the experts use during the peer review process.

7.2.1.3 Peer Review Knowledge Base It is very clear that in addition to the peer review documentation provided by the notifying country, the eIDAS regulation and its implementation acts need to be followed during the peer review by the experts. However, the documentation may not always be clear and/or does not contain all the necessary information

needed for the assessment. There can also be a need for interpretation. Therefore, the author asked the interviewees what kind of documentation and other sources the experts use while peer reviewing the eID scheme in addition to the mandatory and presented documentation. Based on the answers, it is possible to distinguish four main categories of information sources that experts use during the peer review process:

- mandatory documentation
- standards
- optional documentation
- practice

Fig 23 gives an overview of different information sources that experts use to peer review the eID schemes. All sources are not in a document format. Therefore the author uses the term knowledge base. In addition to the eIDAS regulation and its implementation

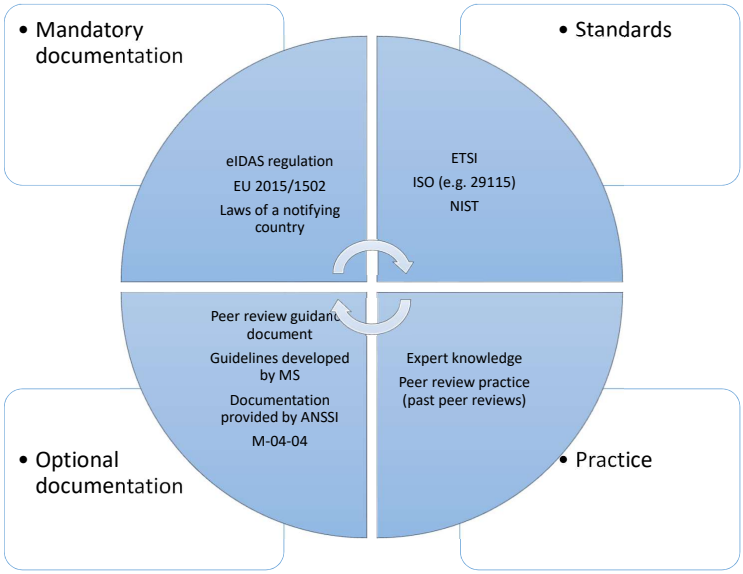

Figure 23: Peer review knowledge base.

act EU 2015/1502, the mandatory documentation contains the legislative acts of notifying countries. One interviewee explained:

> *"If you are active member it means that you are strictly focused on the part of the documentation, may be technology, may be processes in the reviewed member state. In that case, you have to understand law of that country. "*

In addition to the mandatory documentation, the experts rely on optional documentation. The CN has developed a guidance document based on the existing experience to support the CN work. However, the guidance document is optional, and according to one interviewee, the CN members do not always have the same understanding. In addition to the guidance document, some countries have developed their own guidelines for peer review. One interviewee pointed out:

"We have to take the Implementation Act into account, of course, and we have our own technical guideline, and we try to map it to this, of course. "

Some experts use the peer review documentation provided by ANSSI or other organisations dealing with standardization. One of the interviewees explained the background of the LoA levels that come from the United States (US) guidelines "E-Authentication Guidance for Federal Agencies" (M-04-04).[21] The interviewee reasoned:

"But this is the basis, the basis of assurance levels, comes from the this reasoning, and it has actually a long history, that document it's, it's both from the STORK lodge escape pilots back from a memorandum. The US administration, it's M-04-04, where these assurance levels are actually defined. What is an assurance level? And what does it actually mean? And if you would go to 29 115, and you would, I think it's section four is, like this table, it says that assurance level two, which is low in eIDAS terms, it meets this risk profile, this is what you can use it for, the controls are sort of to mitigate the risk to this acceptable levels. "

The aim of the STORK project, mentioned by the interviewee, was to establish a European eID Interoperability Platform enabling the use of national eIDs for cross-border interactions.[22] The same project was followed by STORK 2.0, focusing on identity-related attribute sharing.[23] Document 29 115 referenced by the interviewee is an ISO/IEC standard describing entity authentication assurance framework [65]. This similar framework corresponds to the International Telecommunication Union (ITU) recommendation X.1245 [68]. The same interviewee continued:

"So when I'm evaluating a scheme, I use the guidance, I use the matrix from the ISO standard, and my experience in on what that actually means. sort of have a pragmatic approach. I mean, it's also the national setting that determines what is appropriate or not. "

In addition to the mandatory and optional documentation, the experts rely on different standards. Standards also give a major input to the legislation and form an important basis how to understand and interpret assurance levels. Interviewees mainly brought out ETSI and ISO standards but also standards developed by NIST. One expert explained:

"For instance, I mentioned the remote ID proofing use case. In that case, especially in the beginning, because it was a bit new for everyone. We looked at documentation from NIST, we also sometimes had to look to the last documentation provided by ANSSI in France in order to try to build some kind of rational assessment matrix and to really identify these practices, and also possible vulnerabilities. "

Experts' practical experience also plays a significant role in the peer review process. Several experts mentioned using their own knowledge gained over time to peer review an eID scheme. Moreover, the experts trust each other's expertise in particular areas. One interviewee pointed out:

"The experts know exactly what they have to check. And also, for example, with these kind of questions on the chips, or eIDAS is not my specialty, so I leave it up to them to check if it complies or not. "

[21] https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf
[22] https://web.archive.org/web/20120204134732/https://www.eid-stork.eu/
[23] http://science2society.eu/content/stork-20

Together with the expert knowledge, the interviewees brought out the importance of the previous peer review practice. Considering previous practice helps form a common understanding in certain aspects and ensures more equal peer review of eID schemes. For example, one interviewee explained:

> *"And of course, we take into account the decisions on the past peer reviews. So we do not have documentation on this internally here. Because it wasn´t necessary by now as at least I took part in most of the peer reviews, and somehow had an idea of what we did there in the past. So, we rely on the past documentations and cross checking a bit. "*

To summarize this topic, every expert seems to have his/her own approach, which means that each expert uses, in addition to the mandatory documentation, some other sources that help them in the peer review process. For example, some experts trust more their practical experience, while others prefer to rely more on existing standards and guidelines.

7.2.1.4 Auditing and Certification One of the topics brought out by experts was the role of auditing and certification in the peer review process. The peer review process is not an audit, but just one trust mechanism agreed on by the CN countries on the EU level. Some experts prefer a more formalized and standards-based approach to the peer review process. For example, one interviewee noted:

> *"But I sometimes I would very much like that we have a little bit more of a formal approach. "*

The other interviewee added:

> *"So, we rely on the past documentations and cross checking a bit. But what is also important for us, and I'm not sure if this fits here, but certification as possible reasons to fulfil a requirement. "*

However, some experts believe that every eID scheme is unique, and certification would not help so much to understand the assurance level of a whole eID scheme but can support particular eID scheme components (e.g., chip card-based solutions). One expert explained:

> *"We have to accept that the processes are different. We except that, before the Brexit 30% of the passports in the UK were postal applications and shipped by post. And those passports like electronic identities have been used to open a bank account. The meaning of identification can be different in member states. "*

The other interviewee added:

> *"So, certification plays more mostly a role in the context of chip card based solutions that are easy become comparable, you can take a look on the search certificate and you know, okay, it's fine. That's an easy part. "*

Certification seems to be more important in the case of a high assurance level. One interviewee brought out:

> *"I mean, right now, the normal rules is that you have to show up physically, if you want to register at level high, normal rule is that you have to have certification, the best is your routine, certification. "*

Discussion over the role of certification and its extent is still ongoing in the eIDAS regulation review process. As a result, the experts do not have one view of the topic. However, certification is considered helpful in making some components of the eID schemes comparable.

7.2.2 Levels of Assurance

Three assurance levels, "high", "substantial" and "low" come directly from the eIDAS regulation [42]. In addition, more specific requirements for every particular assurance level are stated in the eIDAS implementation regulation EU 2015/1502 [160]. However, the legal acts do not always cover all aspects related to the eID schemes under peer review, but the experts need to understand if the eID scheme corresponds to the requested LoA requirements. Therefore, the author asked the interviewees what is, in their opinion, the main difference between the LoA "high" and LoA "substantial" schemes. Table 18 summarises the main differences between those two levels brought out by the interviewees.

Table 18: Main differences between the LoA "high" and LoA "substantial"

LoA "high"	**LoA "substantial"**
Identification of a person is 100% sure	Identification of a person is 95-96% sure
Hardware token is required	Hardware token is not necessarily required
Enables access to all public e-services	enables access to the public e-services with LoA "substantial" or "low".
Resistant against high attack potential	Resistant against moderate attack potential
Physical presence is needed during the enrolment	Physical presence is not necessarily needed during the enrolment

In the case of LoA "high", one of the most important components is identification accuracy. The interviewees reasoned as follows:

> *" I would say that level substantial means that you have something that is quite reliable, with strong identification, mobile application etc. You are, I would say, 95 to 96% sure that you have the right person in front of you. And it's fit for nearly all the use cases, like opening a bank account for example, and level "high" would be to be used in context, where you must be absolutely sure that you have the right person in front of you. "*

> *"For high as it has the highest standard we feel that the authentication process must be 100% trustful. For example, we wouldn't allow biometrics or video identification for LoA high, because you don't have, you can't be 100% sure that the outcome is this really true. "*

> *"And level "high" would be to be used in context, where you must be absolutely sure that you have the right person in front of you. "*

> *"For level high, you really have to know for sure that it's the person that he says he is. And that it's secure, and that it's resistant against attacks. "*

Some interviewees found that in the case of LoA "high" user´s physical presence is required. However, the identification accuracy does not actually depend on the user´s physical presence. One interviewee explained:

> *"One is face to face. It doesn't necessarily have to be physical face to face, but it has to be an interaction. Currently, it means actually stepping into the passport office or whatever, and applying and retrieving a eID. So physical presence and face to face presence. "*

In addition to the accuracy, the interviewees brought out important aspects, like having a secure element included in the eID scheme and resistance against attack potential, that makes a difference between assurance levels. The interviewees reasoned as follows:

> *" And for level "high" you need to have a secure element outside of a phone a smart card or SIM card like in Estonia, for example, if I remember we valued the scheme, etc. "*

> *"I would say cryptography. Protection mechanism relying on cryptography and of course but that's more easy to say than to assist. The implementing act on LoA refers to the common criteria and the capacity to resist against attack with a moderate or high potential. But of course, once we start to investigate what high attack potential and all you're supposed to be capable to resist, it gets a bit harder to assess. "*

Another interviewee added that there is also a need for a hardware token. The interviewee reasoned:

> *"The second one is that there is a hardware token. It's sort of it's tamper resistant, and it's something that you carry. I mean, it could be within your mobile phone, but I mean, it's some kind of hardware protection. "*

When it comes to the LoA levels in general, several interviewees mentioned during the interviews that countries mostly try to notify their eID schemes on LoA "high", and other levels are losing their importance. For example, one interviewee pointed out:

> *"When we look at what is happening at the European level, my personal opinion is that everyone wants to go to the level "high" and level "substantial" is losing its value. I am not able to explain what is the purpose of level "substantial" at the level of the European Union today. "*

Another interviewee added that the requirements are quite old and should be reviewed. The interviewee explained:

> *"I think also the substantial level should be reviewed as of the requirements. As the technology develops, I think we cannot base on the same criteria that has been established in 2014, when the implementation act took in force. I think, there has been about 10 years where the documentation and criteria have not been updated. So, I really see that should be reviewed by the Commission. Probably on the Cooperation Network level with the other experts of the member states. "*

Finally, the author asked the interviewees' opinions about the necessity to notify LoA "low" schemes at the EU level. Nine interviewees out of ten said that LoA "low" schemes should not be notified at the EU level for interoperable use. Interviewees reasoned their opinion:

"No. [Name of a country] from the beginning said that we just need the LoA "high" and no differentiation between high and substantial, because that makes it just more complex. But now we have the system, but the voluntary acceptance of the LoA low does not help a lot I think. "

"Honestly, we do not recognize notified schemes that level low. And even in [Name of a country], do not have so many relying party using level low. So for me, it's not that useful. We have enough solution today using two factor authentication. And we can slowly get rid of mono factor authentication. "

"For cross-country authentication. I think LoA low should ´t be included. Depends on, on what you're able to do with a scheme, which is not high but low? "

However, some interviewees found that it should be at least possible to notify LoA "low" schemes. For example, one interviewee noted:

"I think it's good to have this level low, which is for anything else than what is notified. We use it for the private banking, etc. And we also use it in other cases where there's no need to actually notify, but you will need an assurance level that can be used for other things right. "

The other interviewee added:

"Obviously, there is a lot of sort of good and usefulness of low, but I think the politically no one wants to sort of admit that. "

Based on the interviewees' feedback, it is possible to say that experts are able to bring out the main differences between the eID schemes and their LoA levels. However, most experts found that the current classification of the LoA levels does not correspond to the actual need and use of the eIDs in the EU.

7.2.3 Factors Influencing Peer Review

In addition to the organisational and peer review content-specific aspects, the author wanted to know how different social and cultural aspects affect the eID peer review process. Based on the answers, the author was able to distinguish three types of factors:

- personal
- social and cultural
- historical

From a personal perspective, the personal background of experts may influence their preferences and how they participate in the peer review. One interviewee brought out that experts usually have their favorite topics in the peer review process. The interviewee explained:

"And I mean, actually persons not countries, because everyone, as I said, have their own favourite topics or favourite areas. "

Four countries out of nine found that different social and cultural aspects significantly affect the peer review process. The interviewees reasoned their position:

"It does, I mean the national practice is also related to the certification or enrolment for instance. Some member states have a four-eye principle in issuance. Others do not. In particular, if it is a de-centralized system and this particular administrative culture that into the discussions of a peer review where less understanding of the other member states administrative cultures can lead to weird discussions. We do not have that it in other aspects in the common market. "

"A lot. I mean, it's so obvious in all cooperation's, not only within the eID area, within the EU, and there are certain countries that have sort of different positions, different reasoning and different. Well, approach is basically and culture, which is coloured by the culture. And it repeats all over. So I mean, yes, it affects a lot. "

"So, this is specific aspects definitely influenced the peer review regarding what is possible in a state and what is not. For example, is there a register that could be used to central one or is the vendor register that influences the system the possible requirements, the possible commitments that they could made and then directly influences. Also the assessment to be honest because you could not expect the state to provide something he cannot provide. Regarding cultural aspects, I am not a pro on this. So I am not sure but I would expect that they play a role. "

One interviewee explained that some countries may have, for example, strong data protection rules or other principles that are very important for them.

For Another four countries, the social and cultural differences may influence the peer review process but not significantly. Interviewees explained:

"Not too much, I would say. I think countries who have a little different view or how they are implementing their eID in their own country cannot affect too much. Yes, it can affect if you are providing more advanced, let´s say eID with more advanced technology "

"I do not think that so much. Why? Because of we have the clear process. We have a structure for this process. We have clear defined roles and what can be changed according to the not nationality, but culture of that country, it is responsibility may be to deliver all documents, questions-answers on time. Some country has a culture that it is not important to deliver it strictly at that moment. "

"There can be some reflections on like, in some member states, they work a lot with trust, they are trusting the people in the system and other member states are more strict. "

It is important to emphasize that even though social and cultural play a role in the peer review process to some extent, it is not necessarily negative. One interviewee pointed out:

"And I think it's actually for good that we have different cultures and different views on this. It's for the good of everyone, because you need to both be very hold on to your principles, while also looking at different angles and on different levels and all that. So I think it actually is a good thing. It's not bad that we have different cultures and traditions. "

One interviewee found that social and cultural differences do not affect the peer review process. However, the experts may have different opinions inside the peer review group. The interviewee explained:

" I don't really see in a in a peer review group, you clearly see like, a difference member states have different ones they find more important. "

In some cases, the size of a societal group may also play a role. One interviewee said there is, and has always been, a gap between big and small countries in the EU.

When it comes to the historical aspects, some interviewees brought this aspect out separately. For example, interviewees brought out the following aspects:

" So somehow the historic background definitely plays a role regarding, for example, mentioned a couple of times. So hopefully, it's not boring by now. But just so the countries have a different understanding and how to identify people and ponds of register. "

"Probably that between some country where for historical reason, there have been some difficulties? Let's say that people will be more cautious with the question, because there are always some kind of underlying political dimension. "

The interviewees' answers reflect that different factors affect the peer review process, in one way or another, and they cannot be ignored. Some of those factors may have bigger, others smaller influence, but it is important to be aware of them. The author tries to consider these aspects while designing a framework for eID schemes assessment.

8 A Multifaceted Assessment Framework for eID Schemes

This chapter gives a detailed description of the multifaceted assessment framework of eID schemes, hereinafter also named eIDAF. Designed framework bases on the data sources and expert input collected during this research on the national and EU level. Research results are validated via additional expert interviews and three scenarios. Exact methodological steps are described in Chapter 2. The author follows the theoretical concept proposed by Koppenjan and Groenewegen and uses process, technological, and institutional design elements in the eIDAF framework. Therefore, the author describes separately processes, roles, responsibilities, and regulatory framework that supports the assessment activities. The author focuses on two major use cases. The main framework presented in fig 24 is suitable for the assessment of the EU and EEA countries´ eID schemes. The second use case, presented in fig 25, reaches beyond and covers the eID schemes assessment activities between any two countries.

According to the current practice, the eID scheme peer review follows the same process regardless of the declared assurance level. At the same time, every LoA corresponds to the different requirements and provides important indications about a particular eID scheme. However, depending on their declared LoA, the trust mechanism and recognition processes are different. Therefore, the author finds that the experts should focus mainly on the assessment of LoA "high" eID schemes. This tendency was also mentioned during the interviews.

One possible way for the CN is to peer review only LoA "high" eID schemes and enable listing/notification of LoA "substantial" and "low" eID schemes at the EU and EEA levels. Of course, in this case, the existing peer review procedure needs to be overlooked, and clear notification requirements to be provided. Principles coming from the eIDAS regulation are applicable in the EEA countries. However, every country has its own right to define its national processes for the eID schemes used inside the country. Therefore, the author does not focus on this layer more in-depth during this research.

Fig 24 gives a general overview of the eIDAF model that could be used for the eID schemes assessment at the EEA level. According to the figure, every country has its own nationally recognised eID scheme or schemes provided by the public sector or private sector authority.

When a country would like to use its eID scheme across borders, it is important to understand the LoA of a particular scheme. The legislative framework, together with applicable forms and guidelines, help the country to describe the eID scheme according to the requested LoA level. Depending on the LoA level, the eID scheme will be peer-reviewed or notified. According to the fig 24, the peer review process is only for the eID schemes requesting LoA "high". LoA "substantial" and "low" schemes will go through a simplified notification process guided by the EC. After the notification process, the schemes will be listed as recognized eID schemes at the EEA level. Recognition of the LoA "high and "substantial" eID schemes would be mandatory and LoA "low" eID schemes voluntary. It means that other countries can accept LoA "low" schemes for interoperable use but are not entitled to do so.

In the case of peer review, the process will be carried out by the CN according to the procedure. After the peer review process, the peer-reviewed eID scheme will be listed as a recognized eID scheme at the EEA level, and other countries must recognise the eID scheme for cross-border interaction.

In both use cases, the EC and the CN exchange information about the eID scheme and communicate with each other whenever expert opinion is needed, etc. It is important for both processes to have a clear process description, documents/forms, and a guidance

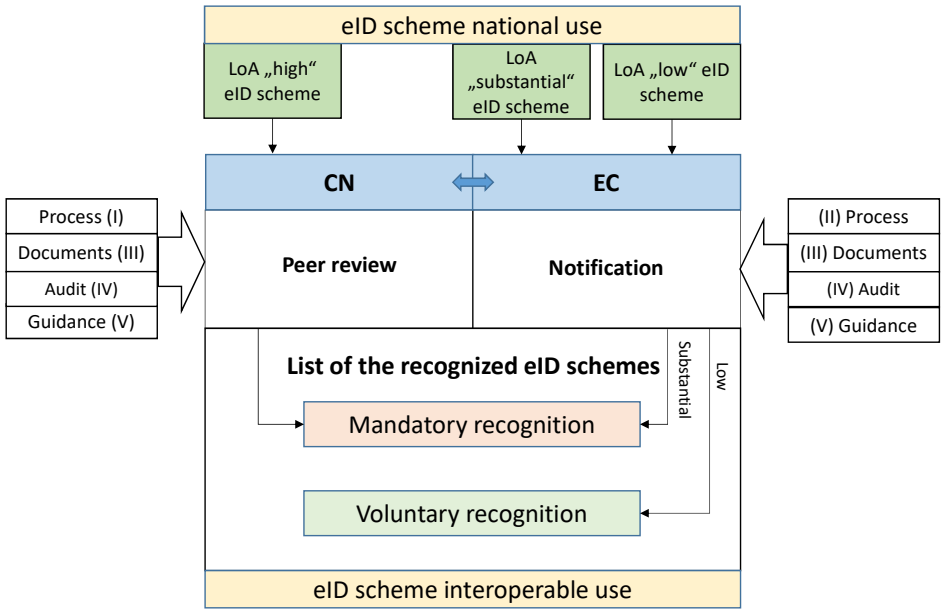

Figure 24: General overview of the eIDAF framework applicable at the EEA level.

document that all involved stakeholders can follow. In addition, previous auditing of the eID scheme and its components provides valuable technical and security-related information to the CN experts and the EC.

During the expert interviews, it was emphasized that peer review should not intervene in the countries' sovereignty. The author also identified that different social and cultural aspects affect the peer review and how countries understand and interpret the LoA requirements. The designed eIDAF model gives flexibility for the EEA countries to decide the acceptance of the LoA levels for interoperable use and enables them to take into account the specifics of a particular country. However, audit results create a solid base and add additional assurance to the peer review process.

A similar framework can be applied between any two countries that would like to start cross-border use of their eIDs. However, in this case, only the peer review process is sufficient to cover all LoAs. However, it is not likely that LoA "low" would be recognized for cross-border use between two countries. Fig 25 presents the peer review model applicable between any two countries outside of the EEA. During the peer review, it is important that both countries follow the same process, documentation, forms, and guidelines for the eID schemes assessment. In addition, the requested LoA level of both countries should be the same. For example, if one country (country A) requests LoA "substantial", then the other country (country B) should be able to correspond at the same assurance level.

Both countries should have an expert group consisting of people covering different competences that enable the evaluation of the eID scheme correspondence to the requested LoA requirements. This expert group can be formed separately, or it can be similar to the group used for checking the compliance of an eID scheme at the national level. The number of experts in the group is not limited. More important is the expertise they cover. It is important that the experts are able to assess the enrolment and identification processes, eID means and their technical components, security aspects, etc. After the peer review, the eID scheme will be listed in the other country as a recognized eID

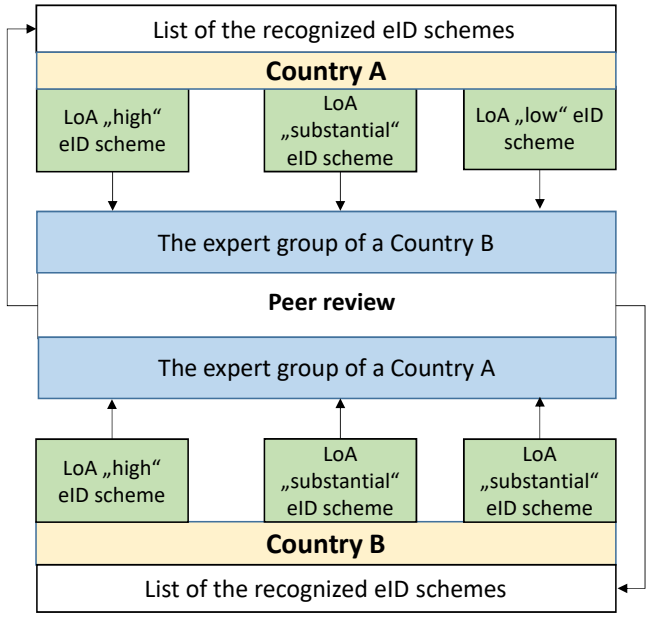

Figure 25: General overview of the eIDAF framework applicable between any two countries outside of the EEA.

scheme, and it is possible to start cross-border interaction.

Another question is how to notify about the changes in already peer-reviewed or notified eID schemes. Currently, there is no special simplified procedure for that. However, the practice has shown that even small changes may significantly affect the whole scheme. Therefore, it is not reasonable to design a separate process for handling changes and modifications in the peer review or the notification process. However, the author agrees that the presented documentation can be, in this case, reduced and could focus on the changes. However, the peer review or notification process would still be carried out as usual.

The author understands that this multifaceted framework will not solve all general interoperability challenges. However, it enables taking the first steps toward the international interoperability framework and allows the building of smaller interoperable communities based on the mutual trust schema.

To successfully implement the framework, it is important to have standardized processes in place. First of all, the process itself needs to be clear and transparent. All involved parties must understand their role and responsibilities. Standardized documentation, forms, and guidelines shall support the process itself. And finally, the eID schemes assessment itself needs to be conducted in a manner that enables clearly distinguishing different LoA levels and comparing them. Therefore, the author focuses on sub-chapters 8.1, 8.2, 8.3 and 8.4 on these aspects more closely.

8.1 Assessment Process

Based on the eIDAF model presented in fig 24, the eID schemes assessment process contains two different processes:

- peer review process for the LoA "high" eID schemes (I)
- notification process for the LoA "substantial" and "low" eID schemes (II)

The author re-designed the peer review process based on the expert interviews and other documentary information collected during the research. According to the re-designed process, the peer review will be carried out by the CN and coordinated by the EC. The EC will manage the notification process. Both processes presume their own standardized forms and guidelines.

8.1.1 Peer Review Process

Before it is possible to make changes in the process itself, it is important to define the stakeholders who participate in the process. Currently, in addition to the representatives of the notifying country, there are the following roles in the peer review process: coordinator, three rapporteurs, active members, and observers.

Based on the interviews, it was clear that the current role division in the peer review process could be more optimal. This is also supported by the fact that it is challenging to cover all these roles by different member states at the CN meeting, especially when there are several parallel ongoing peer reviews.

One way to re-organise the role division and support the peer review process is to make the following changes:

- the EC should coordinate the peer review process. As coordination is more formal and does not necessarily require expert knowledge, it would be a reasonable shift
- the rapporteur role remains the same and will be covered by the CN experts
- there is no need to distinguish active members and observers as those countries who decided not to actively participate in the peer review process automatically become observers and can keep an eye on the peer review process in the EC-provided online environment
- as peer review topics are closely related to each other, it would be more optimal not to divide active members between the topics. When a member state decides to participate in the peer review, then the participation is active equally in all topics

This leads to another aspect, which is topics in the peer review process. Currently, the peer review consists of three topics: enrolment, eID means, and management and organization. Enrolment and interoperability aspects of eID means are definitely topics that need to be checked by experts as every member state practice can be different. Therefore, the experts should be able to assess the eID schemes as a whole in the cross-border context. Management and organisation is a relevant topic and should be included in the peer review process. However, the content of this topic could be covered to a large extent based on the audit results. Fig 26 presents the possible peer review role division. According to the figure, the peer review is coordinated by the EC. The CN members can participate as rapporteurs or active members in the process. However, the rapporteur's role should be divided by at least two EEA countries to ensure the objectivity of the peer review. In the case of parallel peer reviews, it is recommended that the EEA country that has already decided to participate as a rapporteur in one peer review would not take more than an active member role in other peer reviews. This recommendation is based on the practice when in some cases, the experts are very overloaded and unable to contribute as much as they would like, and the quality of the peer review may be affected.

In the case of any two countries, the role division presented in fig 26 can be used. The coordinator will be the authority responsible for the eID schemes description and notification. Rapporteurs and active members should be from various stakeholder organisations. The national legislation shall regulate roles, members, and their responsibilities in the peer review process.

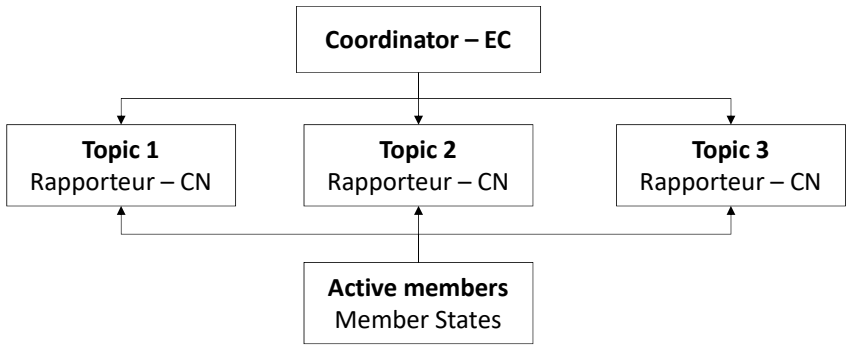

Figure 26: Peer review role division applicable at the EEA level.

Based on the changes in role division, it is possible to reshape the peer review process. However, based on the expert´s feedback, existing peer review steps consisting of three question rounds, one meeting, and three rounds for the report review seem to work relatively well. Therefore, the aim of the author is not necessarily to completely re-design the existing process and propose something completely new but improve the existing process. Before it is possible to talk about the process itself, it is important to understand the peer review indicative time frame.

Based on the collected data, it is reasonable to have the possibility to pre-notify an eID scheme to enable the EC and the EEA countries to have an idea about the eID scheme to be notified. However, the time should not be longer than six months. Therefore, the optimal pre-notification time would be four months. It means between two CN meetings. In the case of any two countries outside of the EEA, the pre-notification process is optional, and the process starts with the document submission. However, between the submission and the first kick-off meeting, experts must have time to familiarize themselves with the documentation.

Four months (16 weeks) for a peer review process is sufficient as every eID scheme is different, and it is good to have some buffer time if additional meetings or clarifications are needed. Indicative peer review schedule and duration of activities applicable at the EEA level and between any two countries is presented in table 19. According to the list of activities, the optimal time to conduct one peer review is approximately 14 weeks. It leaves two weeks buffer time period for unexpected activities.

The improved peer review process applicable at the EEA level is presented in Fig 27. The main difference with the existing peer review process is in activities and the sequence of how they are performed during the peer review. For example, during the first kick-off meeting after the CN meeting, the notifying country should give a presentation about the scheme and introduce the presented documentation so that the rapporteurs and active members have easier to follow the documentation. Currently, the first kick-off meeting focuses more on the peer review schedule and time planning.

Also, there is a difference in activities in the sequence. Currently, rapporteurs start drafting the peer review report after the 3rd question round. However, during the in-

Table 19: Indicative peer review schedule

Activity	Duration
Peer review preparation	2 weeks
Kick off meeting	1 day
1st Q/A round	4 weeks
2nd Q/A round	2 weeks
Meeting	up to 2 days
3rd Q/A round	2 weeks
Peer review report	2 weeks
Report revision	1 week
Preparation for the CN meeting	1 week
Total	**14 weeks**

terviews, it became clear that starting with the drafting earlier would be reasonable, for example, after the 2nd question round. Then it is possible to discuss the first version of the report at the peer review meeting, after which the active members still have a chance to ask additional questions during the 3rd question round and finalize the report. Finally, after the report is ready, the CN opinion draft and presentation will be prepared and presented at the CN meeting.

The author suggests that the first questions and answers round should be longer, two weeks for questions and two weeks for answers because the biggest amount of questions is usually collected during the first round. Following rounds can be already shorter.

One of the topics mentioned by the interviewees was consensus finding. Currently, there is no clear process for solving disagreements inside the peer review group; every case is handled individually. However, recent peer review practice shows that this kind of mechanism is necessary. The author does not have one single solution to overcome the issue. However, one possibility is using a TA toolbox method, where mediation is suggested for problem solving [53]. During the mediation process, a neutral third party will be used to overcome the situation. In the peer review context, the neutral party can be a group of member states (for example, representatives from three countries) that do not participate in the peer review process or an independent EU institution. There can also be a separate permanent structure in the CN responsible for consensus finding and solving disagreements arising from the eID schemes notification and their interoperable use. However, the mediation mechanism should be agreed upon between the member states and described separately.

The final decision about the eID scheme LoA level, its correspondence to the eIDAS, and its implementation acts requirements will be taken at the CN meeting. The results will be published in the Official Journal of the European Union. After the successful peer review process, the EEA member states should recognise the eID scheme for cross-border use cases.

When it comes to the international practice and peer review process between any two or more countries, then the peer review role division is much simpler. Peer review will be carried out by the national expert group consisting of competences from different authorities (identity management and identity proofing, security, technology, etc.). The expert group has a leader responsible for peer review coordination. The process itself can follow the same logic as presented in Fig 27 under the "eID scheme peer review" sub-chapter. However, the peer review results will be presented at the meeting between the two countries, and the eID scheme will be approved and listed for cross-border use

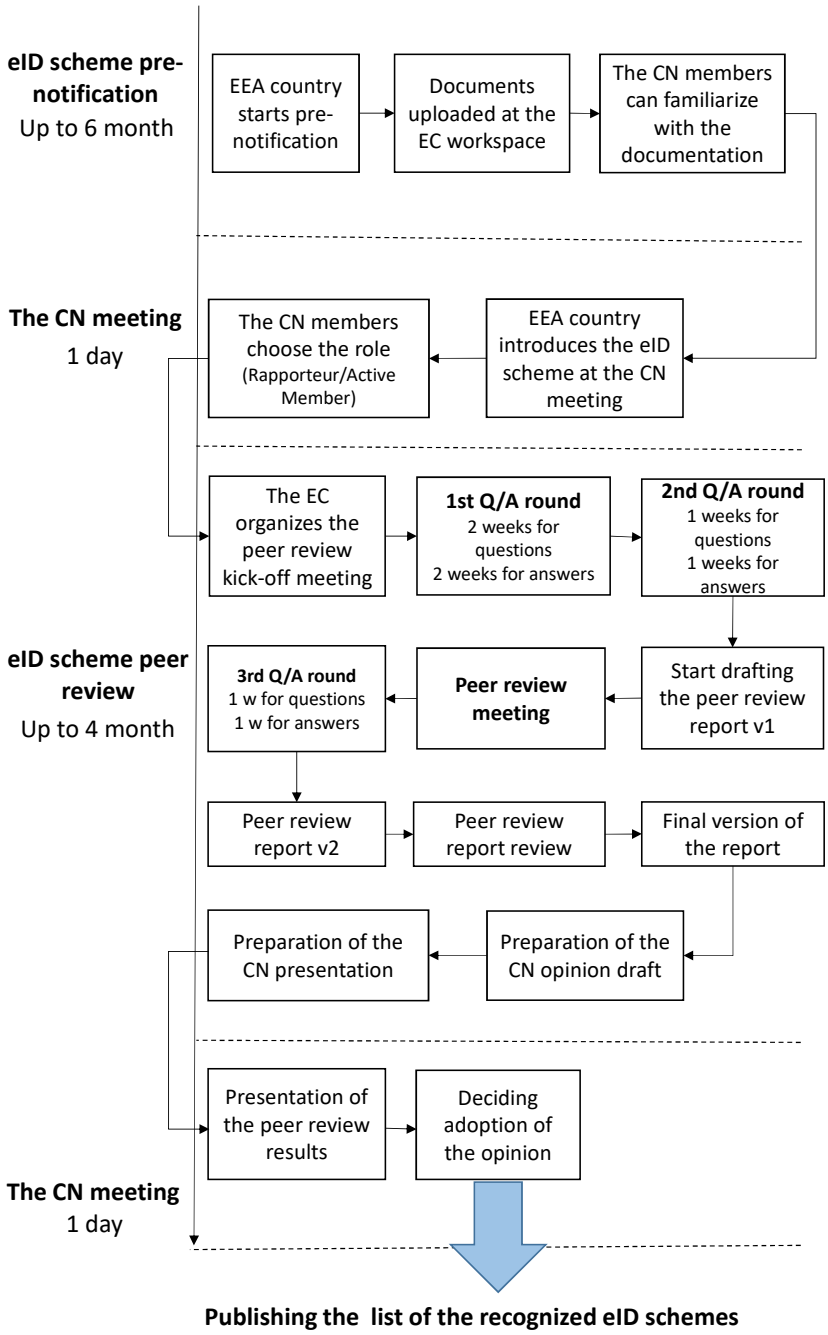

Figure 27: Improved peer review process applicable at the EEA level.

according to the national regulations.

Pre-notification of the eID scheme is not separately necessary. When a country submits its documentation, the other country should have time before the kick-off meeting to familiarize themselves with the documentation. The overall time for the peer review

would be, in this case, also four to six months. As this peer review between the two countries covers all assurance levels, then the notification process is not applicable and is only for the EEA countries.

8.1.2 Notification Process Proposal

The notification process as such does not currently exist. However, it is one way to simplify the existing eID scheme's peer review process at the EEA level. Therefore, the author describes one possible way for the notification process. Pre-condition for the notification is that the country has assessed the eID scheme and its LoA at the national level. Then it is possible to prepare notification documentation and present it to the EC.

The EC does not have special competence to evaluate the provided documentation. Therefore, the interviewees suggested engaging an independent third party to review the documentation. For example, the European Union Agency for Cybersecurity (ENISA) could check whether the provided documentation is accurate and corresponds to the declared LoA requirements. It is possible to argue if it is necessary to check the submitted documentation, and theoretically, the EC could do that by itself. However, as it is possible to notify two different assurance levels ("substantial" and "low"), it would be good to have an independent expert opinion on whether the documentation corresponds to the requested LoA requirements or not. Moreover, the ENISA can give valuable suggestions and recommendations during the process that improve the security of the eID schemes under the notification. The overall process could take up to two to three months.

When the notification documentation is complete, then the EC lists the eID scheme as notified, and it can be accepted for interoperable use. When the documentation is not sufficient, the EC returns the documentation to the notifying country with feedback. The country can then decide whether to change the documentation and submit it again or cancel the notification process. Fig 28 represents the possible notification process. As a result of the notification process, the EEA countries have a certain time frame (for

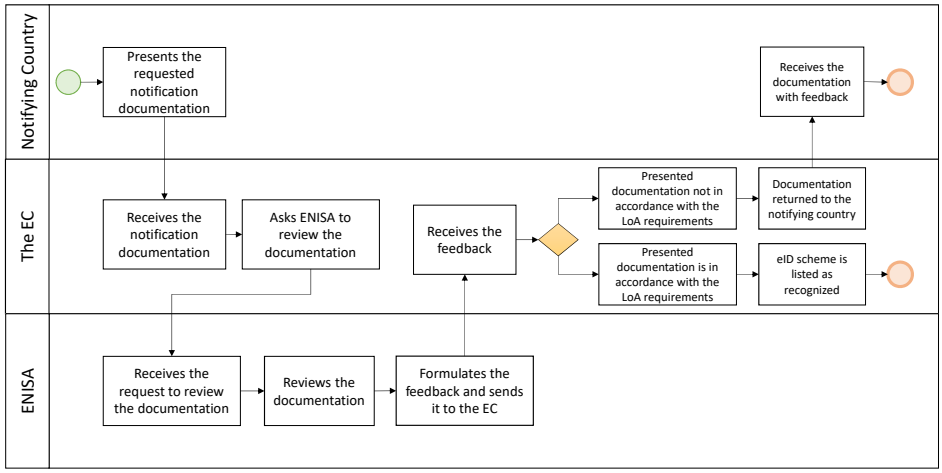

Figure 28: eID scheme notification process applicable at the EEA level.

example, 2 to 3 months) to decide whether they accept the notified LoA "low" scheme. In the case of LoA "substantial", the recognition is mandatory. Information about the countries that have accepted the scheme for interoperable use will be presented together with the list of the recognized eID schemes.

The notification process is EEA-specific. Therefore, it is not applicable internationally, where all LoA levels are equally peer-reviewed.

8.2 Assessment Documentation

Another important aspect is the documentation and information needed from the notifying country for the LoA assessment. In this chapter, the author focuses on the documents part (III), presented in fig 24.

The duration of the peer review process and the effort that the experts need to invest in the peer review depends on the quality and organisation of the data provided by the notifying country. Currently, the peer review is based on the notification form adopted by the implementation decision (EU) 2015/1984 [159]. However, during the expert interviews, it was clear that every country describes its eID scheme differently, and finding necessary information is not always easy. Countries also often use templates from previous peer reviews and try to modify them according to their scheme.

Moreover, several experts mentioned that too much information about the national processes is presented in the documentation. Therefore, it is important to define the main documents and information needed for the peer review and the notification process. This dissertation aims not to propose concrete documentation form(s) or improve the implementation decision but to define the main blocks and components that need to be presented in the documentation by the notifying country.

Usually, in practice, the documentation consists of following the documents:

- cover letter;
- notification form - a document that contains main information about the eID scheme and is based on the standardized template adopted by the implementation decision [159];
- white paper - a document that gives a general overview of the eID scheme and main procedures;
- LoA mapping - a document that describes how the eID scheme corresponds to the requested level of assurance according to the eIDAS implementation regulation EU 2015/1502 [160];
- any other documentation that the notifying country considers important to add.

Based on the re-designed peer-review process and input from the experts, it is possible to standardize the documentation necessary for the peer review and notification procedure and ease the CN and the EC work. However, it seems that there is no need to distinguish the application documentation between the peer review and the notification procedure, as in both cases, it should be possible to identify fulfillment of the LoA requirements and suitability for interoperable use. Moreover, separate forms would probably create additional complexity and confusion for the notifying countries. Therefore, having one standardized form/template for both processes would be reasonable.

The author proposes that the assessment documentation should contain the following elements:

- cover letter;
- standardized peer review/notification form;
- annexes.

Standardized peer review/notification form should cover at least the following topics:

- Introductory part - name of the scheme, list of eID means, declared LoA level, authorities responsible for the eID scheme, and contact persons of the notifying country.
- Overview of an eID scheme - detailed description of the eID scheme under notification (i.e., enrollment process, authentication, etc.) together with the figure about the overall eID scheme.
- LoA mapping of an eID scheme together with the auditor confirmation- description how the eID schemes meet the requirements of the eIDAS implementation regulation EU 2015/1502 [160] and confirmation of an auditor that described requirements are met.
- Interoperability - gives an overview of how the eID scheme will be operating in cross-border use cases and how the eIDAS interoperability requirements are met.
- Risk assessment - overview of the risks related to the eID scheme (including risks related to the interoperable use of the scheme) and applicable mitigation measures.

Security and data protection are topics that cannot be extracted from the eID scheme. Therefore, these two aspects must be covered under every topic throughout the document. Annexes will be submitted if applicable. Risk assessment is an essential part of the peer review documentation. However, today not always covered. In the peer review context, interoperability-related risks and their possible mitigation measures should be covered in the documentation.

Annexes should contain information about conducted audits and their results, different certifications related to the eID schemes, or other relevant information that the notifying country finds important.

In this case, countries that need to go through the eID scheme receive the information much more concentrated format. Therefore, it is not necessary to duplicate the information in different documents. Moreover, some topics, especially relevant for the assessment, like interoperability and risk assessment, are separately brought out. This, on the one hand, reduces the experts' workload, but on the other hand, it reduces the number of issues that need to be clarified during the question rounds.

However, due to the scope of this dissertation and the number of details that need to be specified to improve the existing notification format template, the author remains on a general level. This general documents list can be taken as a basis to re-design the standardized format for the eID schemes peer review and notification in the next stage of the research. The author agrees that it is probably possible to present the same information within the existing notification format. However, in practice, those topics are not always sufficiently covered or not presented in a well-organised way.

When the standardized notification format is updated/re-designed, it can be used at the EU level and generally between any two countries that want to use their eID schemes for cross-border service provision.

8.3 Auditing and Certification

Auditing and certification is a topic that causes a lot of discussions at the EEA level. Experts have different opinions, and countries have various positions when it comes to the topic. Sometimes it is even hard to follow the discussions as people mix those terms or do not

distinguish them properly. Therefore, this chapter focuses on the audit (IV) part of the fig 24. More specifically, the author analyses and tries to understand how and to what extent the certification could be used in favor of the peer review and the notification process.

One of the most challenging parts of the eID scheme peer review process is forming a reasoned opinion about the correspondence of the eID scheme to the requested LoA requirements. Existing legal regulations define general principles that need to be followed during peer review. However, every expert is different and interprets the presented documentation differently depending on his/her background and experience. Moreover, expert interviews revealed that the CN experts use various other sources while peer-reviewing an eID scheme in addition to the mandatory documentation that needs to be followed.

According to the interviews, the core components of an eID scheme are the enrollment process, authentication factors used, interoperability aspects, and security. All these four domains are broad and cannot be covered by one standard or regulation. Based on the interviews and according to the EU legal practice, the author tried to understand different fields and aspects that are and/or should be covered during the eID scheme peer review process and how these fields are connected to the different legal acts and standards. The findings are summarized in Fig 29. However, the figure does not cover all possible applicable standards but gives some examples of applicable standards.

During the peer review process, it should be possible to assess the eID scheme technical solution (technology), processes related to the eID scheme relevant to the cross-border service provision, interoperability solution, and security and privacy aspects of the eID scheme. Currently, the eIDAS [42] and its implementation regulation [160] cover most of these aspects. However, security concerns could be more covered by the EU Cybersecurity Act (CSA) [161] and privacy and data protection concerns by the GDPR [43]. Furthermore, in March 2022, the EU Agency for Cybersecurity (ENISA) published an analysis of standardization requirements in support of cybersecurity policy, also specifying the EU legislative acts related to risk management [167].

In practice, the legal environment does not provide a complete list of requirements necessary for the eID schemes assessment. Therefore, the experts need to use other sources (standards, guidelines, previous practice, etc.) to fill the gaps. Moreover, most of the CN experts are not specialised in security matters. This has led to discussions among experts on how to use existing standardisation schemes in favor of the peer review process. The aim is not to create a standard for the eID schemes peer review but to analyse to what extent the experts can rely on the certification in the peer review process. Existing standards enable the creation of a certification scheme in the security domain, and that is what ENISA is doing together with the European Cybersecurity Certification Group (ECCG) inside the EU cybersecurity certification framework [161]. However, this certification scheme is much broader and to be applicable in a particular case should cover the specifics of the eID schemes.

Ideally, the eIDAS implementation regulation should define technical requirements and standards that need to be followed in every LoA supported by the standardized notification form. Then, the notifying country describes how every LoA requirement is met. During the LoA audit, the independent certified auditor will check the correspondence of the described LoA requirements to the actual implementation.

Based on the previously described concept, the author proposes a general model that can be used in the eID scheme peer review process. The model is presented in Fig 30. According to the model, the notifying country describes the eID scheme and performs

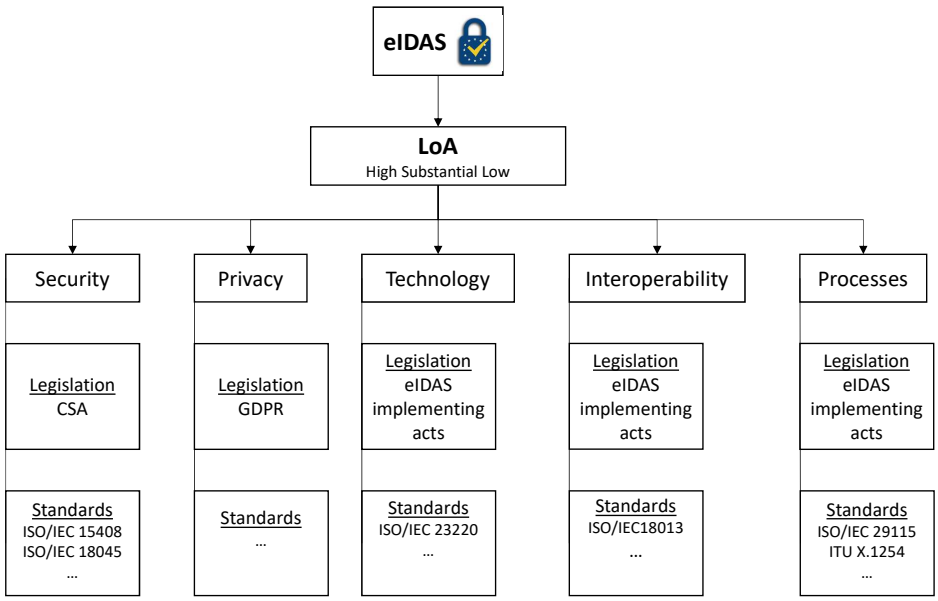

Figure 29: Standards used for the assessment at the EEA level.

an audit using an independent certified auditor. Auditor confirmation will be presented to the CN during the peer review process, together with other relevant documentation necessary for the peer review.

The Cooperation Network conducts the peer review by going through the enrollment processes, authentication factors, interoperability, and security and can ask additional questions to ensure that the eID scheme is proper for interoperable use. The author fully understands that the eID scheme is a complete solution where different aspects are interconnected (e.g., security, data protection, etc.). Therefore, the author believes that an audit helps clarify some general aspects in advance. As a result, the experts have a preliminary understanding of the eID scheme and confidence that the description corresponds to reality. In that case, the experts can focus on the core elements of the peer review. The CN activities during the peer review should base on the legal acts supported by the assessment guidelines.

In the case of the notification process, it is enough when the audit is carried out to clarify the level of assurance "substantial". LoA "low" should not presume any additional auditing. Notification documentation itself is already sufficient for the process.

When it comes to the more general level, two countries can accept eID schemes and audit results. However, in this case, the independent certified auditor should be recognised by both countries.

8.4 Assessment Guidelines

This chapter focuses on the guidance (V) part presented in the fig 24. Usually, the focus in every process is on mandatory documentation and legislative acts. However, the author believes that in the eID schemes assessment, all supportive documents play a significant role and help to maintain the quality of the process and its outcomes. Herefore, guidelines are something that is not written and, after some time, forgotten, but something

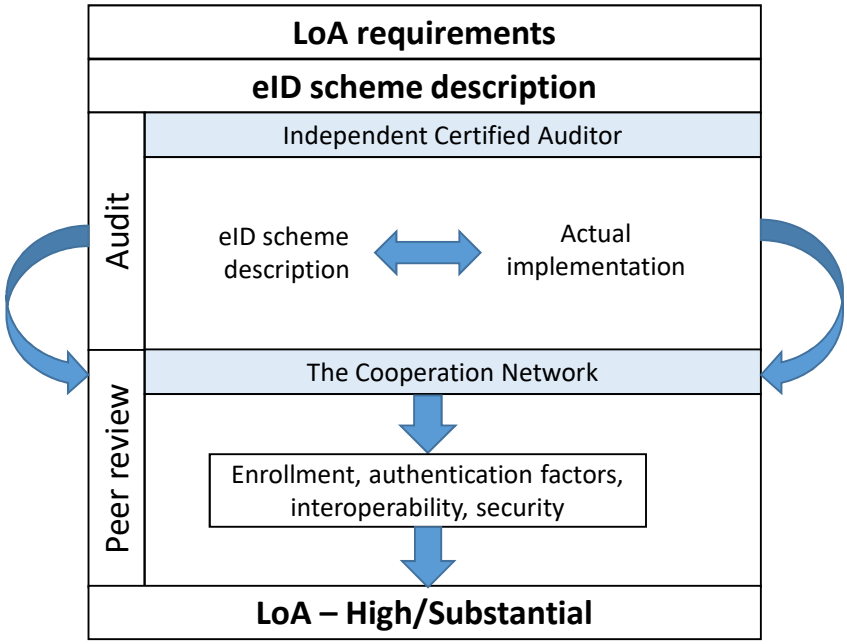

Figure 30: eID schemes assessment model applicable at the EEA level.

that develops over time. The guidance document aims to complement the legislation by providing interpretation when needed and reflecting the latest assessment practice.

Based on the interviews, it was evident that experts rely on different sources, and some countries have developed their own internal guidelines. However, this may lead to a situation where the experts are not able to come to an agreement, or eID schemes are assessed on an unequal basis.

The CN's role is not only to conduct peer reviews but also to exchange practices related to the eID schemes and their cross-border use. Therefore, the CN should also keep the guidance document agile so that it reflects the latest practice and agreements from the previous peer reviews. More specifically, the guidelines should include:

- interpretation and/or explanation of the existing legal requirements (including interpretations provided by the EC);
- suggestion of standards that could be used to peer review an eID scheme or its components;
- practice from the previous peer reviews;
- process-related guidelines (how to handle special cases etc.);
- guidelines for the country that reviews an eID scheme under the notification.

Sometimes, some general questions or concerns are raised during the peer review process. They are not related to the particular scheme but apply to all schemes. In this case, depending on the concrete question, the CN can form an opinion or ask in legal matters interpretation from the EC. These practical activities should be documented and included in the guidelines.

As experts work differently, it is helpful to have a list of standards that are recognized and relevant available. In that case, the experts have a complete set of mandatory and supportive documentation they can rely on. Those standards and full texts could be available in the CEF working environment.

The general peer review process is well described and understandable. However, there are cases that may require a different approach. For example, if it is necessary to make slight changes in the already notified peer review scheme. How to identify if the change is slight? Also, a slight change may significantly affect the whole scheme. The guidance document should provide an answer to how to overcome this kind of issue. Moreover, the guidance document should describe how to act in case of disagreement between the CN members and give a direction on what to do when two or more peer review participants have different opinions about the eID scheme.

The guidance document should also cover topics related to the notification process. For example, the country that receives an eID scheme to overview may have notification process-related or LoA-specific questions.

The most challenging part is probably keeping the guidance document developing and up to date. Therefore, it would be good if every CN member would be responsible for renewing the guidance document, for example, six months. Then it would not be too much of a burden for one country, but there is also someone responsible for making the changes if needed. It also encourages the cooperation between the countries.

9 Initial Evaluation: Expert Interviews

To strengthen the internal validity of the research results, the author conducted three evaluation interviews with the experts who participated in the eIDAF design process. The experts were selected different from the countries used for the scenario-based evaluation to increase the objectivity of the evaluation process. Interviewees were from the following countries:

- Estonia (EE), interview conducted 07.11.2022 10.00-11.00.
- Austria (AT), interview conducted 07.11.2022 15.30-16.30.
- Sweden (SE), interview conducted 08.11.2022 15.00-16.00.

The interviews were conducted online using the MS Teams platform. The interviews were recorded and later transcribed. One hour was planned for each interview. The interviewer introduced the aim and the structure of the interview and informed the interviewees about the recording. The interview aimed to validate the eIDAF framework design with the CN experts who took part in the framework design process and made changes in the framework when needed. The interviewer introduced the following main components of the eIDAF framework to each interviewee:

- General overview of the eIDAF framework applicable at the EEA level.
- General overview of the eIDAF framework applicable between any two countries outside of the EEA.
- Peer review role division applicable at the EEA level.
- Indicative peer review schedule.
- Improved peer review process applicable at the EEA level.
- eID scheme notification process applicable at the EEA level.
- Assessment documentation (sub-chapter 8.2).
- Assessment and certification part (sub-chapter 8.3).

The interviewer wanted to know from the interviewees two things about each introduced component:

- Is the introduced component usable in real-life situations?
- How to improve the introduced component?

Based on the interviewees' feedback, the author modified different components of the framework. The final version of the proposed eIDAF framework is presented in Chapter 8. This chapter provides deeper insight into the expert's feedback and recommendations, as all of them could not be directly implemented. The interviewees brought out valuable discussion points and challenges that need further discussion at the policy-making level.

The interviewer introduced the drafted eIDAF framework applicable at the EEA level as presented in the Fig 31. Fig 31 presents the first proposed version of the eIDAF framework. All interviewees found that the framework is applicable. However, they provided several valuable comments to consider.

One interviewee found that voluntary recognition of LoA "substantial" eID schemes would fundamentally change the eIDAS regulation. The interviewee explained:

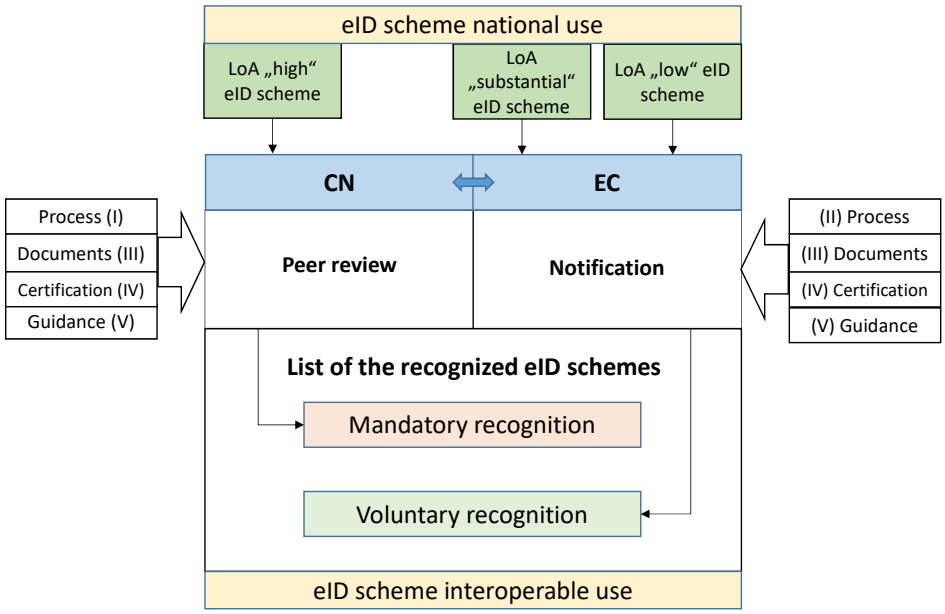

Figure 31: Draft version of the eIDAF framework applicable at the EEA level.

> *"I think this will basically undermine the very foundation of the eIDAS regulation, which is the mutual recognition and the since several Member States rely very heavily on level substantial, this sort of breaks it apart. "*

According to the interviewee, mutual recognition of both assurance levels ("substantial" and "high") is important as the use of e-services at the level "substantial" is much higher than at the level "high".

However, the topic, in general, needs further political discussion at the EC and Member States levels. This statement is supported by the answer from another interviewee, who raised a question about the nature of peer review in general. The interviewee argued whether the peer review is a process with a binding outcome or just a non-binding learning exercise. There is no fully common understanding of this matter among the Member States. Therefore, it is not possible to solve this matter within this dissertation.

Based on the interviewees' feedback, the author of the dissertation decided to change the drafted eIDAF framework by making the recognition of the LoA "substantial" eID schemes mandatory. The renewed framework is presented in the Fig 24.

According to one interviewee, peer review leads to an asymmetric situation where the accountability of the peer-reviewing country is not clear. The interviewee explained:

> *"I could simply say as a peer reviewer just out of the blue without substantiating it, I think it doesn't meet LoA "high". And then, you are in that asymmetric situation other than with certifications or conformity assessments where you have, as a rule that the same product certified by different certification authorities, should lead to the same result. I mean that's theory that's clear, but we formally don't have that in the peer review. And that is what I mean with asymmetric situation that in the peer review scheme that there is nothing hindering a Member State saying, I think that scheme doesn't meet LoA high because I dislike video identification or whatsoever. "*

The interviewee continued:

> *"So we do not have measures to hinder a Member State to make unsubstantiated claims in the peer review. So that is a different levels of powers in the in the peer review there is no independent process, which you have with certifications or conformity assessments where the peer reviewed country could appeal to. "*

According to the interviewee, it is not clear what is the accountability of the countries taking part in the peer review process. This is especially an issue when there is low consensus between the countries. If the peer review is binding, then there should be a possibility to appeal.

The author of the dissertation agrees that there should be a separate process to handle claims and to achieve consensus between the countries. The procedure itself should be described in the assessment guidelines. According to the existing practice, the claims are taken at the CN meeting level, and the final decision is made there. However, as the meetings take place 3-4 times a year and are planned for about one hour for every peer review results presentation, the CN members may not have enough information and time to make well-considered decisions. As a solution, the author sees that the consensus-finding process should be separately described in the guidance document enabling the CN to involve independent third parties (e.g., ENISA) when needed. The author proposes one possible process model for consensus finding in Chapter 8.

The interviewees made no further comments about the general overview of the eIDAF framework applicable between any two countries outside of the EEA presented in Fig 25. One interviewee brought out that it is very good to describe this process in advance as there are actual cases (e.g., Ukraine, Israel, Singapore) that need to be handled.

The author introduced the peer review role division applicable at the EEA level presented in Fig 26. All interviewees found it applicable and useful. No suggestions were made to change the proposed role division. One interviewee explained:

> *"To reflect and confirm your own approach to this, that I find this very efficient or for comparing with the approach we have or the practice we have today at the Commission level where it doesn't make sense in a way because. Very often, the rapporteurs and the coordinators can overlap sometimes or have to overlap for some reason, because the peer review organization is fine, is having hard times finding those rapporteurs so and first hand, the coordinators should not overlap with other roles so. I would have to say that this will resolve most of those issues. "*

Another interviewee found that it is good to have the EC as a coordinator. The interviewee reasoned as follows:

> *"In particular, having the EC as a coordinator makes sense because then you have comparable situations between the peer reviews. "*

The author introduced the indicative peer review schedule presented in table 19. The interviewees found the schedule reasonable and made no changes. However, one interviewee suggested that a more rigorous way to fill in the documentation would speed up the procedure. This comment also supports the author´s proposal to standardize the assessment documentation.

After the peer review schedule, the author explained the improved peer review process applicable at the EEA level as presented in Fig 27. The interviewees found the process applicable and gave some general comments. One interviewee pointed out that it may be hard to start drafting the peer review report before having the full picture of the eID

scheme. However, according to the proposed process, the drafting of the report starts after the second questions round, where usually the most urgent questions are already clarified. Therefore, the author did not change the proposed sequence of activities. Another interviewee came back to the need to have a clear consensus-finding process in place. The author supports the idea. However, this does not presume changes in the particular schema.

The author introduced the draft version of the eID scheme notification process applicable at the EEA level as presented in Fig 32. Interviewees found the process valid and gave valuable feedback. One of the interviewees proposed that instead of the EEA country, the

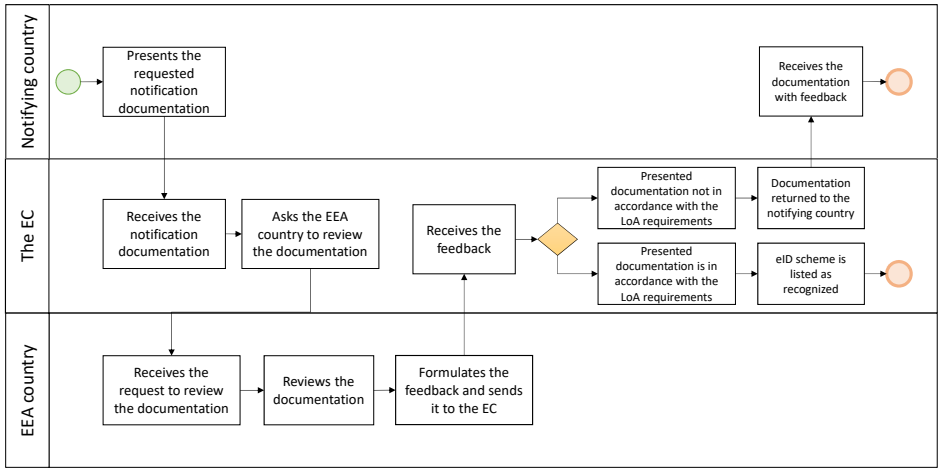

Figure 32: Draft version of the eID scheme notification process applicable at the EEA level.

eID scheme could be reviewed by ENISA. The interviewee explained:

> *"For me, the question would be could instead of EAA Country also have ENISA for instance role in being independent and not having own states? [...] So ENISA is an EU agency that anyhow has a task to assist Member States in the Commission in technical aspects. You have a more independent review than just speaking one Member State."*

The author agrees that it would be more objective to have an opinion from an independent third party. Therefore, the draft version of the scheme will be changed accordingly.

According to the other interviewee, the submitted documentation must be accompanied by an additional third-party audit report. The author agrees with the principle, and therefore, assessment documentation is analysed more in detail in sub-chapter 8.2.

The interviewee introduced the peer review documentation necessary for the eID scheme LoA assessment. The author proposed that the assessment documentation consists of three main documents: a cover letter, a standardised notification form, and annexes. Standardized notification form should contain an introduction, eID scheme overview, LoA mapping, interoperability, and risk assessment parts. Interviewees found the proposal sensible and made some additional comments. One interviewee brought out that the notification should contain information about the private sector relying parties referring to the eIDAS article 7F [42]. Otherwise, the interviewee found that the proposal covers all important aspects necessary for the peer review. Another interviewee argued

if interoperability should be a part of the peer review process. The interviewee explained as follows:

> *"[...] interoperability part is sort of mandatory to fill in from some aspects in the pre-notification. But the peer review is not focused there and it is the wrong people. I for example am not part of the technical subgroup. So I have no idea about the SAML[24] profiles and the attributes releases and all that type of things. So I think it is actually misplaced. I don not think it belongs in the peer review. "*

According to the interviewee, interoperability is not part of the peer review process, and all the CN experts may not have enough competence to evaluate it. The interviewee also pointed out that there are no security requirements on the eIDAS nodes. Based on the other interviews, interoperability was mentioned as an essential component. Moreover, the eIDAS implementing regulation states that the aim of the regulation is to ensure interoperability when mapping the national assurance levels of eID schemes [160]. Therefore, the interoperability aspect should be covered in the peer-review documentation. Another thing is how and to what extent and how it should be evaluated. Based on the interviewees' feedback, the author made slight changes in the peer review documentation proposal presented in sub-chapter 8.2.

Finally, the author presented the draft eID schemes assessment model applicable at the EEA level, showing the extent to which the certification could be used in favor of the peer review process. The draft of the model is presented in Fig 33. The author is aware that the topic is challenging and causes discussions in the CN and at the EU level. Therefore, the author was ready for contradictory feedback. However, the received comments were constructive and helpful.

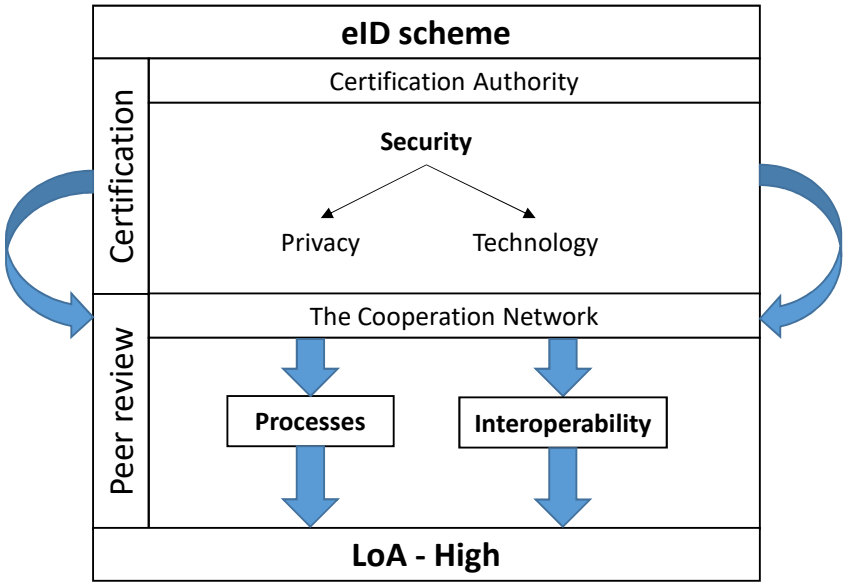

Figure 33: Draft eID schemes assessment model applicable at the EEA level.

[24] Security Assertion Markup Language

One of the interviewees brought out the data protection perspective and wanted to know the role of the Cooperation Network on certified data protection aspects in relation to Article 42 of the GDPR, as the national data protection authorities are responsible for it. The author agrees that the CN's role is not to evaluate data privacy concerns. As a result of the discussion, it is clear that the concern is not only data privacy-specific. It is important to understand what is actually in the scope of a peer review and how far the CN experts can go in the process. During the design phase, the author mapped the main peer review components. According to the Fig 21, the peer review consists of four main components: enrollment, interoperability, authentication factors, and security. The author believes that those components can be taken as a basis while defining the peer review scope.

Another interviewee found the technology certification challenging. The interviewee explained:

> *"[...] I think certification of technology is a challenge because you actually need to have the detailed defined the requirements on the technology, and it is usually just boils down to. Ok, we can do this with smart cards because they look exactly the same in different countries. But once we get into like mobile phones and apps and all that FIDO tokens and what not, then this war is lost basically. You can't really set this detailed requirements at four different technologies, because they simply work so different ways. "*

According to the interviewee, a proper certification scheme presumes many criteria and work, and by the time it is agreed upon, the technology is already developed elsewhere. However, that does not exclude the possibility of having reliable independent third-party auditors and a general approach to the certification topic.

The interviewee proposes a solution where the notifying country fills in a notification form similar to the LoA mapping document and explains how the eID scheme works. An independent recognized auditor would then audit the provided description to determine whether the LoA description corresponds to reality. The author agreed with the comments and updated the drafted eID schemes assessment model applicable at the EEA level. The modified assessment model is presented in Fig 30.

All interviewees supported the idea of having guidelines. This is one way of preserving collective memory. To benefit from the guidelines the most, it should be a recurring task to keep it up to date. Moreover, one interviewee pointed out that the status of a guidance document should be clear. Otherwise, the guidance would be followed selectively.

The author offered the interviewees an opportunity to add any other comments or suggestions at the end of the interview. Overall, the interviewees did not find major concerns regarding the presented framework. They rather tried to bring out some aspects that should be considered or included as an improvement to the framework. One interviewee concluded:

> *"[...] I'm looking forward how and when this process and the proposal would be adopted by the Cooperation Network and the Commission. So I think it's a very valuable work you have done for the Cooperation Network and regarding the evaluation of the ID schemes, there's much more clarity in this now as I see it visually. And I hope I hope this will find practice in in future. "*

10 Scenario-Based Evaluation

This chapter focuses on the evaluation of the research results. The author uses a descriptive evaluation method based on three scenarios suitable for the DS research framework [60]. A detailed description of the evaluation method and its selection criteria is presented in sub-chapter 2.4.

Selected scenarios reflect the eID scheme peer reviews of Denmark, the Czech Republic, and the Netherlands. The CN experts from those three countries have accepted the use of their eID scheme peer review practice as a scenario. Moreover, the selected countries reflect the latest peer review practice and bring out different challenges. However, the author remains on a general level and will not go into technical details due to security reasons and taking into account that some parts of the eID scheme may be covered with patented technologies or contain business secrets of private companies that cannot be publicly available. Taking into account political reasons, the author also does not connect certain concerns, opinions, statements, or participation information to particular EEA countries.

Every scenario description contains at least following information:

- name of the eID scheme;
- notified eID means;
- requested LoA level;
- general overview of the peer review participants;
- overall duration of the peer review;
- peer review process description (timeline);
- documents presented in the peer review process;
- main challenges;
- applicability of the eIDAF framework.

After presenting the main characteristics of the eID scheme, the author focuses on the process and content analysis by describing how the peer review was conducted, what were the main challenges and how the peer review would have been carried out in the eIDAF framework. The author focuses on the following aspects:

- applicability of the eIDAF model;
- possible role division;
- indicative duration;
- process analysis;
- documentation analysis;
- applicability and analysis of the assessment model.

10.1 Scenario 1: Denmark

Denmark notified its eID scheme NemID first time in 2019 at the level "substantial". The CN published an opinion about the NemID scheme in January 2020. There are 6 different eID means (key card (OTP), mobile app, key token (OTP), NemID hardware, Interactive Voice/Response (OTP), Magna key card) operating under the NemID scheme.

In 2021, Denmark started the notification of their eID scheme MitID. This scenario focuses on the analysis of the MitID peer review process. Under the MitID scheme following eID means were notified:

- mobile App;
- app enhanced security;
- chip;
- code display;
- audio code reader;
- password.

The requested LoA levels of the MitID schemes were substantial and high. In total 9 countries participated in the Danish peer review as active members in at least one of the three topics. Six countries took only the observer role. In topic one, "Enrollment" there were 7 active members and 6 observers. In topic two, "eID means management and authentication" there were 9 active members and 6 observers, and in topic three, "Management and organisation" there were 4 active members and 8 observers.

The peer review started in December 2021, and the CN opinion was formed in June 2022. The overall notification duration of the MitID notification process was about six months.

Denmark started their eID scheme pre-notification at the end of 2021. The Danish MitID scheme was introduced on 21.02.2022 at the CN meeting. The first peer review meeting was held on the 8th of March, 2022. Fig 34 presents the overall timeline of the MitID peer review. In addition to the activities presented in the fig 34, during the period 08.03.2022-14.06.2022, the peer review team had weekly meetings and in May and June additional meetings to clarify some specific issues. The peer review report was presented at the CN meeting on 27.06.2022.

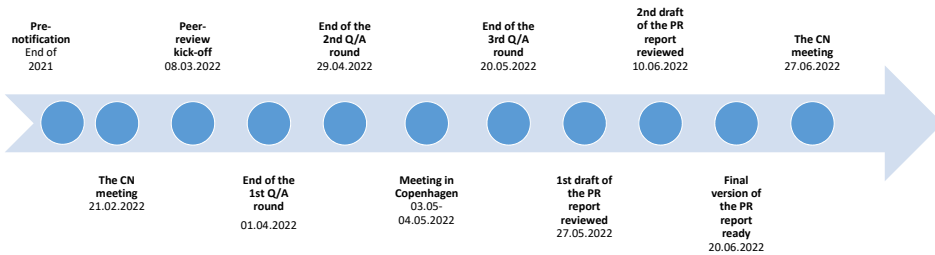

Figure 34: Danish eID scheme peer review timeline.

The MitID notification documentation consisted of following documentation:

- notification letter;

- LoA mapping;
- White paper;
- 30 supportive documents/annexes;
- 11 additional documents.

The notification letter, LoA mapping, and the white paper, together with 30 other documents and annexes, were presented during the pre-notification phase. Eleven additional documents were presented during the peer review process.

During three question rounds, in total, 157 questions were asked. Most of them are related to topics 1 and 2. Only five questions were asked about the management and organisation.

The most challenging topics in the MitID peer review process were the video enrolment process (risks related to the attacks by video injection) and concerns related to the chip (use of the chip with known vulnerability in the MitID scheme). These concerns are also reflected in the Cooperation Network opinion No 5/2022 [157].

The MitID solution was notified at "substantial" and "high" levels. However, according to the opinion, Denmark commits to take different actions (i.e., monitor risks, perform additional testing, phase out the existing MitID chip, assess the security of the chip) to ensure the highest level of assurance [157].

It is possible to apply the eIDAF model to this scenario. However, in this case, the amount of material to be peer-reviewed would decrease, as all information related to the LoA substantial (in total, four eID means) would be handled separately in the notification process. Only one solution (MitID App together with the chip) as a whole was notified at the LoA "high".

From the roles point of view, the peer review would be led by the EC, not by the EEA country, and the peer review group would have consisted only of active members without division between the three topics. The estimated duration of the peer review would be 4 to 6 months, taking into account the reduced amount of material to be reviewed. Previously conducted LoA audit would probably have reduced the number of questions asked during the peer review.

The peer review process follows more or less the same pattern. However, according to the proposed process, the first draft of the peer review report would have been ready by the face-to-face meeting. Currently, the main discussion started after the second question round during the actual meeting. As a result, it was necessary to agree on additional meetings to clarify essential topics at the end of the peer review process, making it even more intense. Therefore, the proposed process change, where the report drafting starts before the peer review meeting, would have clarified many issues beforehand and made the process flow much smoother.

The experts relied on eIDAS and its implementation regulation during the peer review process. However, it was clear that the legislation provides general direction but does not help to solve particular security-related technical concerns. This statement is also supported by the peer review group findings (additional testing, risk monitoring, chip changing, etc.) reflected in the opinion [157]. The previous audit of the MitID solution would have given valuable information to the CN experts and eased the security-related discussions.

Part of the Denmark eID scheme corresponding to the LoA "substantial" would have gone through the notification process led by the EC. After the review by ENISA, the eID

scheme would have been considered as notified or returned with the feedback to Denmark by the EC for further revision. The overall notification process would have been two to three months, which is significantly shorter than a peer review.

To summarize the analysis of the DK peer review scenario, it is possible to say that the proposed multifaceted framework for eID schemes assessment is applicable in this case. Moreover, the analysis indicates that the process would be more efficient and, in some parts, shorter.

10.2 Scenario 2: Czech Republic

The Czech Republic (CZ) notified their national identification scheme on the LoA "high" in 2019. In 2021, the Czech Republic started notification of two new eID means Mobile eGovernment key" (MEG) and "mojeID" under the national eID scheme. Requested level of assurance in case of MEG was "substantial" (one means) and in case of mojeID from "low", "substantial" and "high" depending on the way of authentication (in total 4 means, one "low", two "substantial" and one "high").

The Czech Republic initiated the pre-notification process in mid of September 2021. The new CZ eID means were presented at the CN meeting on the 27th of September 2021. According to the peer review agreement, the peer review report had to be finalized by 04.02.2022. The peer review report was presented on 21.02.2022 at the CN meeting. During 19.10.2021-04.02.2022, the peer review team had weekly meetings to monitor the peer review progress and discuss open topics. In total, 113 questions were asked during three question rounds. 33 questions were asked regarding topic 1, 77 questions regarding topic 2, and three questions were addressed within topic 3. Fig 35 presents the CZ peer review timeline and main activities. Due to the COVID pandemic, the main peer review meeting was held online. The overall duration of the peer review was a bit less than six months.

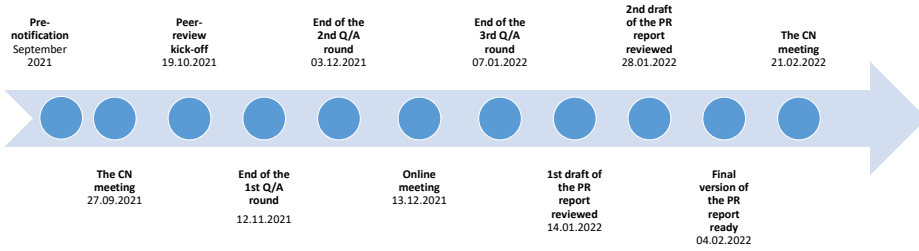

Figure 35: The Czech Republic eID scheme peer review timeline.

In addition to the peer review coordinator, the CZ peer review had seven active members and rapporteurs. Four countries decided to participate as observers.

During the peer review process the CZ presented following documentation:

- notification letter;
- notification form;
- White paper (MEG);
- white paper (mojeID);
- LoA mapping (MEG);

- LoA mapping (mojeID);
- 4 supportive documents/annexes;
- 1 additional document.

All these documents, except one, were submitted during the pre-notification phase. On the 21st of February 2022, at the Cooperation Network meeting, opinion No. 2/2022 was adopted confirming the MEG assurance level "substantial" and mojeID assurance levels "low", "substantial", and "high" [155]. In the case of the CZ peer review, only one concern was brought out in the opinion. It was related to the Data Mailbox Information System as a part of the eID scheme. Historically, the Data Mailbox was used to activate the MEG and mojeID. However, the peer review group did not find the solution resistant enough to the attack potential corresponding to the requested level of assurance. According to the opinion, the CZ commits to ask from all existing and new MEG and mojeID holders additional identity proofing using another eID means corresponding to LoA "substantial" or "high" [155]. Only then, the MEG and mojeID can be used across the borders. The CZ shall inform the CN about the implementation progress [155].

In the case of the CZ eID scheme, the proposed eIDAF framework is applicable. However, the scheme combines different LoA levels that need to be looked at separately. The CZ LoA "high" scheme should go through the peer review process, and LoA "substantial" and "low" schemes should go through the notification process. However, as the CZ already has the information about all eID means under the notification, they can divide the existing information between the requested forms. The author admits that in this case, the notifying country has a bit more work in the beginning to prepare the necessary documentation. However, it makes the further peer review process and notification process more smooth.

The LoA "low" notification process does not presume any confirmation by the auditor. The LoA "high" and "substantial" schemes presume auditor opinion. The CZ case illustrates well how different eID means under one peer review process make the whole process more complex. Therefore, it is more clear when every LoA is described and notified/peer-reviewed separately. Under the same LoA level can be one or more eID means.

In the CZ peer review, it was challenging to form a peer review group and find member states who take the coordinator role. According to the proposed role division, the peer review would be coordinated by the EC with no need to find an EEA country to volunteer. There would not be a separation between the active members and observers and their division between the topics.

The peer review would fit in the fourth-month time frame as proposed. Moreover, there will probably be fewer questions due to the separation of the schemes between the peer review and the notification process. Most likely, additional meetings would not be needed during the peer review process as the experts start forming the peer review report before the meeting. This change in the process enables the experts to address the most important questions during the meeting, and the third question round would be just for minor clarifications if needed at all. The notification process of "low" and "substantial" level schemes could run in parallel with the peer review process and would take 2 to 3 months.

Documents would be submitted according to the standardized forms as proposed. That makes experts' work much easier. The documentation would also contain the auditor's statement that the presented technical solution is implemented as described. In that case, the CN and ENISA experts can rely on the presented information and focus on the technology assessment aspects of their expertise.

Based on the CZ scenario analysis, it is possible to say that the proposed eIDAF framework is fully applicable in this case. Moreover, the process would be much more optimized, allowing experts to focus on their main areas of expertise.

10.3 Scenario 3: the Netherlands

The first eID scheme of the Netherlands (NL), called "Trust Framework for Electronic Identification", was notified in 2019 on LoA "substantial" and "high". The opinion about the scheme was published in the official journal of the EU 13.09.2019 [152]. Shortly after that, the Netherlands notified their eID scheme DigiD in 2020. The opinion about the scheme was published in the official journal of the EU 21.08.2020 [153]. On the 21st of February 2022, at the CN meeting, the Netherlands informed the CN about the changes in their existing eID schemes (the Dutch Trust Framework - eHerkenning/Digidentity and DigiD) to be peer-reviewed. The changes concerned Dutch Trust Framework (eHerkenning/Digidentity) remote identification solution and DigiD application. The requested level of assurance in both cases was "high". According to the NL, the changes were not major, and the CN accepted to have a light version of a peer review. However, from the procedural perspective, there is no process described for a "light" peer review. Therefore, this scenario focuses on the Netherlands eID scheme ´s latest updates and how the "light" version of a peer review was conducted.

Fig 36 presents the NL peer review timeline and main activities. The peer review documents were made available in the mid of April 2022. The first kick-off meeting was held on 16.04.2022, followed by weekly meetings. Instead of three question rounds, there were two question rounds in total. During these question rounds, 56 questions were asked in total. Most of the questions were related to topics 1 and 2. Topic 3 received the least questions (7 questions in total). This pattern clearly shows that the management and organisation topic is not actually very active, and the same tendency can be noticed in other peer reviews.

01.06.2022, the online workshop was conducted. After the online meeting, the peer review group started to draft the peer review report. The first peer review draft was ready by 18.06.2022. The whole peer review process was quite intense, and therefore, there was no time to review the report for several rounds as usual. The peer review results were presented on the 27th of June at the CN meeting. The peer review period was about 2,5 months, from 15.04.2022 to 27.06.2022.

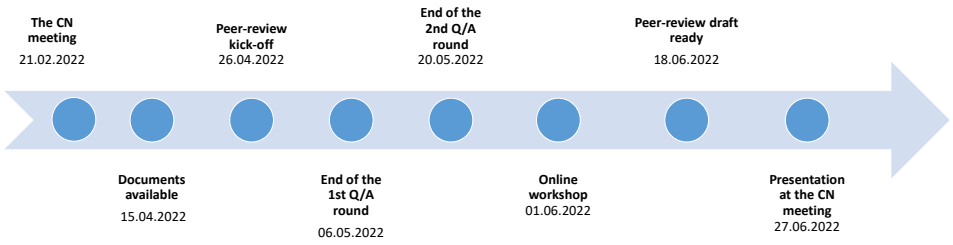

Figure 36: The Netherlands eID scheme "light" peer review timeline.

In total 8 countries participated in the Dutch peer review as active members or rapporteurs on at least one of the three topics. In addition, two countries took the observer role. In topic one, "Enrollment", there were 7 active members and 2 observers. In topic two, "eID means management and authentication", there were 8 active members and 2 observers, and in topic three, "Management and organisation", there were 3 active mem-

bers and 2 observers.

The Dutch peer review documentation consisted of the following documentation: DigiD documentation:

- the CN meeting presentation;
- White paper;
- LoA mapping;
- 2 supportive documents

Dutch Trust Framework (eHerkenning/Digidentity) documentation:

- LoA mapping;
- 7 supportive documents;
- 3 additional documents.

Due to the "light" format, the peer review documentation did not contain a notification form, and the focus was only on the changes. In the case of eHerkenning and Digidentity, three additional documents were presented during the peer review process.

On the 27th of June 2022, the CN formed an opinion about the Dutch eID scheme "DigiD" and found that the eID scheme meets the LoA "high" requirements [156]. During the peer review process, the peer review group was not able to come to a conclusion regarding the changes in the Dutch Trust Framework (eHerkenning/Digidentity), where the full remote video identification procedure was introduced. The peer review group was not convinced that the fully automated video identification solution meets the requested LoA and brought out several security-related risks and its resistance against attackers with high attack potential. Therefore, the peer review countries did not reach a consensus on whether or not the changes introduced by the Netherlands in the eHerkenning/Digidentity scheme comply with the eIDAS regulation and it's implementing act. As a result, the NL continues activities regarding the eHerkenning/Digidentity scheme to correspond to the LoA "high" according to the eIDAS regulation.

At the CN meeting, where the NL peer review results were presented, several member states concluded that the peer review was a bit too intense and more confusing as the "light" form of the peer review was not described. In addition, experts suggested that even some small changes may have a remarkable effect on the whole scheme. Therefore, in some cases, a full peer review is necessary.

The proposed eIDAF model is applicable in the NL scenario. As the requested LoA was "high", the peer review would have been conducted. In this case, the procedure would have been more transparent for the experts, and there would have been more time to go through the proposed changes and ask questions.

The EC would have coordinated the peer review, and eight countries that participated in the peer review would have been active members.

The peer review would have been longer, probably about four months. However, the current peer review, conducted within 2,5 months, enabled the experts to decide only on the DigiD scheme, and the peer review group could not come to a consensus regarding the changes in the eHerkenning/Digidentity scheme. Therefore, the longer peer review period in this particular case would have been justified.

The peer review report was formed at the end of the peer review, and the expert did not have time to go through the report multiple rounds. In the case of the proposed peer

review procedure, the first draft report would have been ready by the time of the online meeting on 01.06.2022. In that case, the experts would have had more time to discuss the video identification solution and make suggestions to be addressed at the CN meeting.

The presented documentation focused mainly on the changes in the eID scheme. However, it made it more complex to understand the whole scheme. Moreover, the countries who took part in the "light" peer review were not the same who participated in the previous peer reviews in 2019 and 2020.

Finally, in this peer review, the previous audit report would have been beneficial, enabling the CN experts to focus on the essential discussions regarding using the full remote video identification solution in the eID scheme.

In conclusion, the proposed multifaceted framework would have been applicable in the case of the Dutch peer review. The scenario shows the importance of a clearly defined peer-review procedure and documentation describing the eID scheme under the notification.

11 Limitations

Every research has systematic biases that are out of the researcher's control. Therefore, it is important to understand, describe and analyse them as they may affect the research results. This research has two types of limitations. Firstly, there are general limitations related to the EU policy-making processes that do not depend on the researcher. These general limitations include EU digital strategies, changes in the use of technology at the EU level, and changes in the legislative environment related to the interoperable use of electronic identities. The second limitation group is associated with this particular research and its activities. However, none of the mentioned limitations make the research results unusable or do not diminish their importance.

From the general limitations point of view, eIDAS and its implementation is a broad topic covering various fields (technology, security, data protection, etc.). When the author of the dissertation planned the research activities, the eIDAS regulation was mandatory, and several member states were implementing it. However, the implementation was challenging for most of the countries. This logically leads to the review of the regulation by the EC and a proposal for a European Digital Identity framework. Therefore, it is important to understand that this research was conducted when the eIDAS regulation was under review. Many principles were under discussion and about to change. There was no clarity on the future role of the peer reviews and the role and responsibility of the CN. It was not clear if the peer review in the existing format was needed at all. The experts discussed possibilities to bring standardization and auditing routines in the eID schemes assurance level assessment. From that perspective, it was challenging to plan the research activities and keep the data and information about recent developments up to date. Only the fact that the author was a part of the CN made it possible to keep up with the pace.

Even now, the debates over the eIDAS regulation text are ongoing. The latest compromise version of the regulation is sent to the European Parliament to be discussed within the year 2023. Before the approval of the final version of the regulation, it is not possible fully to rely on it. Moreover, even if the regulation is adopted, the implementation acts need additional time to be approved. Therefore, the author had to rely mainly on the existing eIDAS regulation and its implementation acts in force while taking into account the latest developments coming from the eIDAS review process. As a result, the proposed multifaceted framework for the eID schemes assessment remains on a level that enables its integration into the new eIDAS concept. Moreover, the legislative process outcome allows further development of the proposed framework.

In addition to the eIDAS regulation, other developments at the European level may affect this research. For example, EU Cybersecurity Act introduces the cybersecurity framework for information and communication technology area products, services, and processes[25]. Furthermore, with the Cybersecurity Act, the EU Agency for Cybersecurity (ENISA) is mandated to develop the EU-wide cybersecurity certification framework. As this research showed, security is an essential component in eID schemes that is complex to evaluate. Herefore, developments in this domain and the creation of an EU cybersecurity certification framework help to clarify the security requirements for eID scheme assurance levels. Moreover, the CN experts do not always have specific expertise to decide whether the solution is resistant enough against high attack potential.

In parallel with the security aspects, the eIDAs regulation changes need to align with the General Data Protection Regulation (GDPR). Personal data processing is an essential part of any eID scheme. However, the CN experts do not have the competence and mandate to evaluate and make decisions on data protection matters.

[25] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

Despite the rapidly changing EU political and legislative environment, the author of this dissertation has tried to take some of the future developments into account while proposing the multifaceted assessment framework for eID schemes, for example, by bringing the ENISA role in the notification process and analysing the role of auditing and certification in the eID schemes assessment. Therefore, the author believes the constantly changing EU legal framework has positively challenged this research and forced it to integrate the most recent changes in the proposed framework.

When it comes to the limitations related to this particular research, the proposed multifaceted assessment framework is developed based on the input of the CN experts only. Therefore, they may have a one-sided view and understanding of the eID schemes assessment process. On the other hand, the assessment of the eID schemes is a very specific domain, and the number of experts dealing with the area is limited. For example, auditing companies that perform the eIDAS audits focus on the trust services part of the regulation, and authentication schemes are not in their scope. Moreover, the EC does not have separate expertise and relies on the CN's opinion. Therefore, this research is based on the best possible competence available in this field. To ensure the highest quality in the research, the CN experts were carefully selected, considering their previous experience and active participation in the peer review process. Furthermore, the author tried to take into account also the geographical distribution of experts. However, the countries in southern Europe have not been that active in the latest peer reviews.

Validation of the research results is one essential component of the DS. This research uses two types of validation procedures. The inner validity of the proposed multifaceted assessment framework was validated through qualitative interviews. The CN experts, who were engaged in the design process, provided valuable input during the validation process based on what the author made changes in the initial outcome. In addition, the author used scenario-based evaluation to ensure the proposed framework is applicable in actual use cases.

The experts evaluated the proposed framework applicable at the EEA level. The scenarios represent the peer review practice of the three European countries. However, the proposed framework should be applicable between any two countries outside of the EEA. From that perspective, the research validation activities could have included qualitative interviews with the third-country eID experts or hypothetical scenario descriptions. Analyzing the pros and cons, the author found that engagement of third countries in the evaluation process would not have created additional value from the research perspective. Mutual recognition of the eID schemes between any two third countries is not a common practice. Therefore, it is hard (if not impossible) to find third-country eID experts with experience with the eID scheme assessment for interoperable use.

Moreover, the publicly available descriptions of the third-country eID schemes (including technical details) are not sufficient to be used for the scenario. Nevertheless, the author believes that validating the eIDAF at the EEA level based on the three positive scenarios confirms the framework's applicability. In case of the interest of any two third countries, it would be interesting to apply the framework. However, this can already be considered part of future research activities.

12 Future Research Perspective

The assessment of eID schemes is a complex and multi-layer topic. Therefore, one of the challenges of this research was the determination of the scope. To meet the research objectives, the author had to remain more general. However, some of the topics covered in the dissertation deserve further in-depth research. Therefore, the author sees more practical activities in the upcoming phases of the study. These practical activities include developing standardized forms for the peer review and the notification process, analyzing the standards and technical requirements applicable at the particular assurance level and developing the assessment guidelines. These activities presume additional interviews or workshop(s) with the CN experts and the EC officials. Moreover, the standardization and auditing topic requires deeper analysis and further discussions with the CN experts and eIDAS auditors.

The research results were validated at the EEA level using expert interviews and descriptive scenarios. However, it would be interesting to research the application of the eIDAF principles in third countries or the applicability of the framework in the case of an EEA member and a third country. Therefore, future research activities should include a case study of the eIDAF framework implementation in a third country.

In addition to the follow-up activities arising from this research, the future research perspective includes upcoming changes in the EU digital identity framework. The eID field in Europe is currently changing fast. The eIDAS regulation, together with its implementation acts, is under revision. In June 2021, the EC published a proposal to amend the eIDAS regulation and drafted a framework for a European Digital Identity [165]. Currently, the discussions over the proposal are ongoing. The compromise proposal is sent to the parliament by the EC. The estimated adoption of the regulation is at the end of 2023. However, in parallel with the legislative process, the EC has initiated various activities to support the fast and effective implementation of the European Digital Identity (EUDI) Wallet. As the initiative is new and under discussion, the author provides a short overview of the solution and the future research perspective in chapter 12.1.

12.1 European Digital Identity Wallet

This chapter focuses on the development of the EUDI Wallet to be established under the regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 regarding establishing a framework for a European Digital Identity [165]. The author relies only on publicly available sources and is fully aware that the final outcome may differ from the concept presented here as the solution and the legislative environment are still under discussion. However, the author believes it is an important upcoming development in the eID field and its interoperable use and therefore deserves closer attention. Moreover, the main concept and idea behind it are unlikely to change.

The EC supports the user-centric approach and a technical solution that enables users to have better control over their data (identity-related information, attributes, and other credentials). Therefore, the EUDI Wallet is one way to implement a self-sovereign identity (SSI) based solution. However, SSI is not just a change in the use of technology but a paradigm shift in the field of electronic identity [118]. This phenomenon separately needs further research in the context of technology acceptance and assessment. Especially how this paradigm affects the countries where people expect proactive e-service delivery from the public sector authorities. Moreover, it is important to understand how SSI-based thinking co-exists in parallel with other data processing principles like the once-only principle [168].

According to the EC staff working document "Impact Assessment Report" provided together with the EUDI framework regulation proposal, the most favorable policy option is a creation of a personal digital identity wallet [164]. Fig 37 presents the possible EUDI ecosystem, where the user decides the provision of his/her digital identity attributes [164]. In practice, the European Digital Identity enables users to open a bank account, request medical certificates, rent a car using a digital driving license, etc.

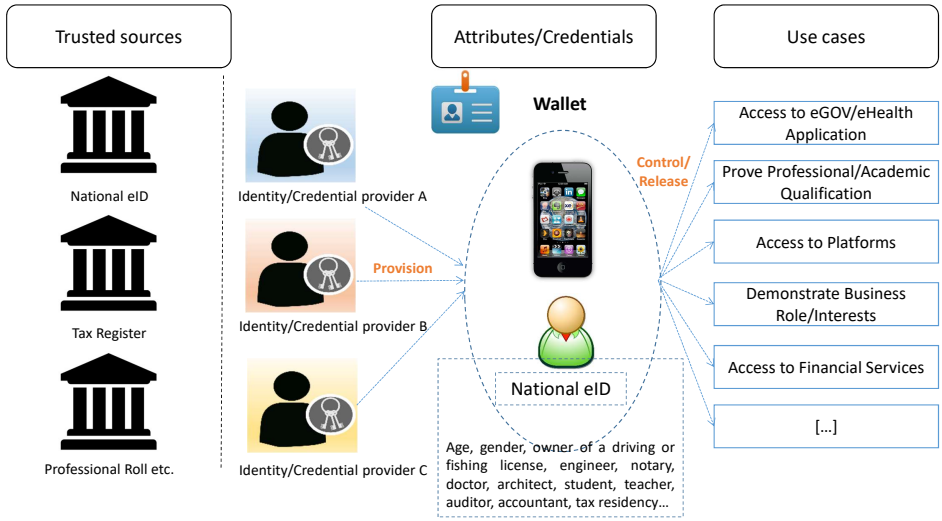

Figure 37: Preferred option for European Digital Identity Ecosystem. Source: The schema is entirely taken from Impact Assessment Report [164].

To support the EUDI Wallet development, the EC adopted on the 3rd of June 2021 a recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework [163]. According to the recommendation, the member states should increase cooperation and create a Toolbox for the EUDI framework. This toolbox should contain a technical architecture and identify a set of common standards and technical references together with the best practices and guidelines to ensure successful implementation of the EUDI framework [163].

The eIDAS Expert Group, consisting of member state experts, has developed an EUDI Wallet architecture and reference framework (ARF) in cooperation with the EC. The first version of the EUDI ARF was published in February 2022 [40]. The concept has been developed further, and the eIDAS Expert Group adopted the final document in January 2023. These ARF documents will be taken as the basis while developing an EUDI Wallet reference implementation. The ARF document aims to provide specifications needed for the development of an interoperable wallet solution taking into account common standards and practices [40].

The aim is to support the EUDI Wallet implementation all over the EU and carry out Large Scale Pilots (LSPs). According to the EUDI Wallet Consortium (EWC) 14.12.2022 press release, the EWC was selected by the EC to participate in the LSP and ensure the EUDI Wallet implementation and its interoperable use[26]. During the pilot, the EWC focuses on three main building blocks of the EUDI Wallet - traveling use case, payments, and organi-

[26] https://eudiwalletconsortium.org/

sational digital identity (ODI)[27]. As a result, four consortia were awarded by the EC to carry out LSPs:

- EUDI Wallet Consortium (EWC) - focusing on mobile travel payments and ODI[28]
- NOBID - focusing on payments issuance and acceptance[29]
- POTENTIAL - focusing on electronic Government services, account opening, SIM registration, Mobile Driving Licence, remote qualified electronic signature", and electronic prescription use cases[30]
- DC4EU - focusing on educational and social security field use cases[31]

The EC has published the European Digital Identity project materials in its official GitHub[32].

However, the implementation of Europe-wide technical projects is always complex and challenging. Therefore, future research activities include an analysis of the EUDI Wallet ARF and the LSP project activities. Therefore, it is important to understand the technical and social challenges related to the EUDI Wallet implementation and evaluate the EUDI Wallet using the technology assessment approach.

[27] https://eudiwalletconsortium.org/
[28] https://eudiwalletconsortium.org/
[29] https://www.nobidconsortium.com/
[30] https://www.digital-identity-wallet.eu/
[31] https://www.dc4eu.eu/
[32] https://github.com/eu-digital-identity-wallet

13 Conclusion

This dissertation summarizes four years of academic research and expert knowledge collected during 16 years in the field of eID at the national and EU level. The author analyzed national eID practices, eIDAS implementation challenges, and the peer review process of eID schemes. This research aims to facilitate the interoperable use of eIDs by proposing a multifaceted framework that enables the assessment of the eID schemes according to their level of assurance. The larger goal is to contribute to developing the EU internal market. Therefore, the research focuses on interoperability to enable cross-border e-service delivery in the EEA and beyond.

To meet the research objectives, the author engages three theoretical concepts (identity theory [25], institutional design by Koppenjan and Groenewegen [80], technology assessment [54]) that help to frame this complex and multi-layer research. Moreover, the author analyses the electronic identity-related academic literature at the national and EU level and uses various qualitative and quantitative data collection methods within the design science framework to propose the multifaceted assessment framework for eID schemes - eIDAF.

This research is the first academic work analyzing in-depth the working routines and processes of the Cooperation Network, which is responsible for peer-reviewing eID schemes at the EEA level. The research is conducted in an exciting and challenging period while the EU electronic identity-related principles are under consideration and about to change. Despite this, the author believes that the result of the research is valuable for the European Commission while reshaping the EU electronic identity field and related legislative framework by providing a more organized approach to the eID schemes assessment. In addition to the detailed work process analysis, the research includes information about the factors affecting the assessment of the eID schemes.

Moreover, the research results enable an interoperable trusted electronic identity scheme between any two countries. However, the author knows that many aspects still need more detailed research. Therefore the author of this dissertation believes that the proposed assessment framework is the first step toward the global electronic market.

List of Figures

List of Tables

References

[1] G. Aavik and R. Krimmer. Integrating digital migrants: Solutions for cross-border identification from e-residency to eidas. a case study from estonia. In *International Conference on Electronic Government*, pages 151–163. Springer, 2016.

[2] R. K. Ahmed, M. H. Khder, S. Lips, K. Nyman-Metcalf, I. Pappel, and D. Draheim. A Legal Framework for Digital Transformation. *International Journal of Electronic Government Research (IJEGR)*, XXXX.

[3] R. K. Ahmed, S. Lips, and D. Draheim. eSignature in eCourt systems. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pages 352–356. IEEE, 2020.

[4] R. K. Ahmed, K. H. Muhammed, A. O. Qadir, S. I. Arif, S. Lips, K. Nyman-Metcalf, I. Pappel, and D. Draheim. A legal framework for digital transformation: A proposal based on a comparative case study. In *the 10th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2021, pages 115–128, Cham, 2021. Springer.

[5] A. M. Al-Khouri. Identity management in the age of mobilification. *Internet Technologies and Applications Research*, 2(1):1–15, 2014.

[6] Á. Alonso, A. Pozo, J. Choque, G. Bueno, J. Salvachúa, L. Diez, J. Marín, and P. L. C. Alonso. An identity framework for providing access to fiware oauth 2.0-based services according to the eidas european regulation. *IEEE Access*, 7:88435–88449, 2019.

[7] A. Alonso, A. Pozo, A. Gordillo, S. López-Pernas, A. Munoz-Arcentales, L. Marco, and E. Barra. Enhancing university services by extending the eidas european specification with academic attributes. *Sustainability*, 12(3), 2020.

[8] O. Amola, S. Lips, and D. Draheim. *Designing a Crisis Management Mobile Application Solution in Nigeria*, page 571–579. Association for Computing Machinery, New York, NY, USA, 2021.

[9] N. Andrade, S. Monteleone, A. Martin, et al. Electronic identity in europe: Legal challenges and future perspectives. Technical report, Joint Research Centre (Seville site), 2013.

[10] N. N. G. d. Andrade. Towards a european eid regulatory framework. In *European data protection: In good health?*, pages 285–314. Springer, 2012.

[11] N. N. G. d. Andrade. Legal aspects. In *Electronic Identity*, pages 1–39. Springer, 2014.

[12] J. Andraško. Mutual recognition of electronic identification means under the eidas regulation and its application issues. *AD ALTA: journal of interdisciplinary research*, 7(2), 2017.

[13] S. Arteaga and I. Criado. From technology diffusion to social use: The case of the eid card in spain. In *Proceedings of the 12th European Conference on eGovernment*, page 66, 2012.

[14] Austria, Estonia and The United Kingdom. *Guidance for notification under the eIDAS Regulation*. European Commission, 2021.

[15] D. Berbecaru, A. Atzeni, M. De Benedictis, and P. Smiraglia. Towards stronger data security in an eid management infrastructure. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pages 391–395. IEEE, 2017.

[16] D. Berbecaru and C. Cameroni. Atema: An attribute enablement module for attribute retrieval and transfer through the eidas network. In *2020 24th International Conference on System Theory, Control and Computing (ICSTCC)*, pages 532–539. IEEE, 2020.

[17] D. Berbecaru and A. Lioy. On integration of academic attributes in the eidas infrastructure to support cross-border services. In *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*, pages 691–696. IEEE, 2018.

[18] D. Berbecaru, A. Lioy, and C. Cameroni. Authorize-then-authenticate: Supporting authorization decisions prior to authentication in an electronic identity infrastructure. In *International Symposium on Intelligent and Distributed Computing*, pages 313–322. Springer, 2019.

[19] D. Berbecaru, A. Lioy, and C. Cameroni. Electronic identification for universities: Building cross-border services based on the eidas infrastructure. *Information*, 10(6):210, 2019.

[20] D. G. Berbecaru, A. Lioy, and C. Cameroni. Providing login and wi-fi access services with the eidas network: A practical approach. *IEEE Access*, 8:126186–126200, 2020.

[21] D. G. Berbecaru, A. Lioy, and C. Cameroni. On enabling additional natural person and domain-specific attributes in the eidas network. *IEEE Access*, 9:134096–134121, 2021.

[22] 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, *Electronic Participation*, pages 41–53, Cham, 2020. Springer.

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

[24] B. P. Bruegger and H. Roßnagel. Towards a decentralized identity management ecosystem for europe and beyond. In D. Hühnlein, H. Roßnagel, C. H. Schunck, and M. Talamo, editors, *Open Identity Summit 2016*, pages 55–66. Gesellschaft für Informatik e.V., 2016.

[25] P. J. Burke and J. E. Stets. *Identity theory*. Oxford University Press, 2009.

[26] S. A. Butt, S. Lips, R. Sharma, I. Pappel, and D. Draheim. Barriers to digital transformation of the silver economy: Challenges to adopting digital skills by the silver generation. In *the 14th International Conference on Applied Human Factors and Ergonomics*, AHFE 2023. Springer, 2023.

[27] C. Calhoun. *Social Theory and the Politics of Identity*. Wiley-Blackwell, 1994.

[28] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, and J. Garcia-Blas. Federated identity architecture of the european eid system. *IEEE Access*, 6:75302–75326, 2018.

[29] H. D. Clarke, M. Goodwin, M. J. Goodwin, and P. Whiteley. *Brexit*. Cambridge University Press, 2017.

[30] C. Codagnone, G. LIVA, and T. R. D. L. H. BALLELL. Identification and assessment of existing and draft eu legislation in the digital field. *Study for the special committee on Artificial Intelligence in a Digital Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg*, 2022.

[31] J. W. Creswell. Qualitative, quantitative and mixed methods approaches, 2014.

[32] P. Crocker and V. Nicolau. A secure architecture for electronic ticketing based on the portuguese e-id card. In *European Conference on Cyber Warfare and Security*, page 38. Academic Conferences International Limited, 2011.

[33] C. Cuijpers and J. Schroers. eidas as guideline for the development of a pan european eid framework in futureid. *GI-Edition Lecture Notes Informatics*, 2015.

[34] J. L. Davis. Identity theory in a digital age. *New directions in identity theory and research*, 15(1):137–164, 2016.

[35] N. N. G. de Andrade. Regulating electronic identity in the european union: An analysis of the lisbon treaty's competences and legal basis for eid. *Computer Law & Security Review*, 28(2):153–162, 2012.

[36] N. N. G. de Andrade. Electronic identity for europe: Moving from problems to solutions. *J. Int't Com. L. & Tech.*, 8:104, 2013.

[37] G. De Gregorio. The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, 19(1):41–70, 2021.

[38] M. Decker, M. Ladikas, S. Stephan, and F. Wütscher. *Bridges between science, society and policy: technology assessment-methods and impacts*. Springer, 2004.

[39] B. Edhlund and A. McDougall. *NVivo 12 essentials*. Lulu. com, 2019.

[40] eIDAS Expert Group. *European Digital Identity Architecture and Reference Framework*. The European Commission, 2022.

[41] N. Engelbertz, N. Erinola, D. Herring, J. Somorovsky, V. Mladenov, and J. Schwenk. Security analysis of {eIDAS}–the {Cross-Country} authentication scheme in europe. In *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, 2018.

[42] European Commission. *Regulation 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)*. European Commission, 2014.

[43] European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. European Commission, 2016.

[44] European Commission. *Report from the Commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. European Commission, 2021.

[45] A. Fairchild. The evolution of the e-id card in belgium: data privacy and multi-application usage. In *Sixth International Conference on Digital Society*, 2012.

[46] D. Falcioni, F. Ippoliti, F. Marcantoni, and B. Re. Digital identity into practice: The case of unicam. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 18–28. Springer, 2013.

[47] U. Flick. Triangulation in qualitative research. *A companion to qualitative research*, 3:178–183, 2004.

[48] S. S. García, A. G. Oliva, and E. Pérez-Belleboni. Is europe ready for a pan-european identity management system? *IEEE Security & Privacy*, 10(4):44–49, 2012.

[49] K. Gerakos, M. Maliappis, C. Costopoulou, and M. Ntaliani. Electronic authentication for university transactions using eidas. In *International Conference on e-Democracy*, pages 187–195. Springer, 2017.

[50] G. Goldkuhl. Meanings of pragmatism: Ways to conduct information systems research. *Action in Language, Organisations and Information Systems*, pages 13–26, 2004.

[51] G. Goldkuhl. Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems*, 21(2):135–146, 2012.

[52] Å. Grönlund. Electronic identity management in sweden: governance of a market approach. *identity in the information society*, 3(1):195–211, 2010.

[53] A. Grunwald. Technology assessment: Concepts and methods. In *Philosophy of technology and engineering sciences*, pages 1103–1146. Elsevier, 2009.

[54] A. Grunwald. *Technology assessment in practice and theory*. Routledge, 2018.

[55] H. Hansson. Studying the opportunities of blockchain implementations in electronic transactions compared to the eidas regulations, 2022.

[56] K. Hansteen, J. Ølnes, and T. Alvik. *Nordic digital identification (eID)*. Nordic Council of Ministers, 2016.

[57] A. Heichlinger and P. Gallego. A new e-id card and online authentication in spain. *Identity in the Information Society*, 3(1):43–64, 2010.

[58] A. Hevner and S. March. The information systems research cycle. *Computer*, 36(11):111–113, 2003.

[59] A. R. Hevner. A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2):4, 2007.

[60] A. R. Hevner, S. T. March, J. Park, and S. Ram. Design science in information systems research. *MIS Quarterly*, 28(1):75–105, 2004.

[61] D. Houdeau. Landscape eid in europe in cy2013. *Open Identity Summit 2013*, 2013.

[62] D. Hühnlein. Towards eidas as a service. In *ISSE 2014 Securing Electronic Business Processes*, pages 241–248. Springer, 2014.

[63] I. Iglezakis. Legal issues of identity management in egovernment. *Available at SSRN 2690374*, 2015.

[64] International Organisation for Standardization. *ISO/IEC 15408-1. Information technology — Security techniques — Evaluation criteria for IT security*. ISO, 2009.

[65] International Organisation for Standardization. *ISO/IEC 29115. Information technology — Security techniques — Entity authentication assurance framework*. ISO, 2013.

[66] International Organisation for Standardization. *ISO/IEC 20000-1. Information technology — Service management — Part 1: Service management system requirements*. ISO, 2018.

[67] International Organisation for Standardization. *ISO/IEC 27000. Information technology — Security techniques — Information security management systems*. ISO, 2018.

[68] International Telecommunication Union. *ITU-T Recommendation X.1245. Series X: Data Networks, Open System Communications and Security. Cyberspace Security - Identity Management. Entity authentication assurance framework*. ITU, 2020.

[69] F. Jordan, H. Pujol, and D. Ruana. Achieving the eidas vision through the mobile, social and cloud triad. In *ISSE 2014 Securing Electronic Business Processes*, pages 81–93. Springer, 2014.

[70] S. Joss and S. Bellucci. Participatory technology assessment. *European Perspectives. London: Center for the Study of Democracy*, 2002.

[71] A. Kalja, T. Robal, and U. Vallner. New generations of estonian egovernment components. In *2015 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 625–631. IEEE, 2015.

[72] D. Kalpaktsoglou, C. S. Hilas, and P. Vouroutzidou. Societal trends and implications of the prospective adoption of eids in greece–preliminary findings. *New Horizons in Industry, Business and Education*, pages 331–337, 2013.

[73] D. G. Katehakis, J. Gonçalves, M. Masi, and S. Bittins. Interoperability infrastructure services to enable secure, cross-border, operational ehealth services in europe. In *Proceedings of the 17th International HL7 Interoperability Conference IHIC*, pages 40–51, 2017.

[74] P. Kavassalis. Designing an academic electronic identity management system for student mobility using eidas eid and self-sovereign identity technologies. *EUNIS*, 2020.

[75] K. Kirilova and A. Naydenov. The state of e-government and digital administrative services in the republic of bulgaria. *Business Management*, 2021.

[76] B. A. Kitchenham, T. Dyba, and M. Jorgensen. Evidence-based software engineering. In *Proceedings. 26th International Conference on Software Engineering*, pages 273–281, 2004.

[77] G. Klimkó, P. J. Kiss, J. K. Kiss, et al. The effect of the eidas regulation on the model of hungarian public administration. *Central and Eastern European eDem and eGov Days*, 331:103–113, 2018.

[78] T. Klobučar. Facilitating access to cross-border learning services and environments with eidas. In *International Conference on Human-Computer Interaction*, pages 329–342. Springer, 2019.

[79] T. Klobučar. Improving cross-border educational services with eidas. In *World Conference on Information Systems and Technologies*, pages 932–938. Springer, 2019.

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

[81] M. Kubach, H. Leitold, H. Roßnagel, C. H. Schunck, and M. Talamo. Ssedic. 2020 on mobile eid. *Open Identity Summit 2015*, 2015.

[82] M. Kuperberg, S. Kemper, and C. Durak. Blockchain usage for government-issued electronic ids: A survey. In *International Conference on Advanced Information Systems Engineering*, pages 155–167. Springer, 2019.

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

[84] Y. Lee, K. A. Kozar, and K. R. Larsen. The technology acceptance model: Past, present, and future. *Communications of the Association for information systems*, 12(1):50, 2003.

[85] G. M. Lentner and P. Parycek. Electronic identity (eid) and electronic signature (esig) for egovernment services–a comparative legal study. *Transforming Government: People, Process and Policy*, 2016.

[86] T. Lenz and B. Zwattendorfer. Towards cross-border authorization in european eid federations. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 426–434. IEEE, 2016.

[87] S. Lips, K. Aas, I. Pappel, and D. Draheim. Designing an effective long-term identity management strategy for a mature e-state. In *the 8th Electronic Government and the Information Systems Perspective*, EGOVIS 2019, pages 221–234, Cham, 2019. Springer.

[88] S. Lips, R. K. Ahmed, K. Zulfigarzada, R. Krimmer, and D. Draheim. Digital sovereignty and participation in an autocratic state: Designing an e-petition system for developing countries. In *the 22nd Annual International Conference on Digital Government Research*, dg.o 21, page 123–131, New York, NY, USA, 2021. Association for Computing Machinery.

[89] S. Lips, N. Bharosa, and D. Draheim. eIDAS implementation challenges: the case of Estonia and the Netherlands. In *the 7th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2020, pages 75–89, 2020.

[90] S. Lips, I. Pappel, V. Tsap, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In *the 7th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2018, pages 60–70, 2018.

[91] S. Lips, V. Tsap, N. Bharosa, R. Krimmer, D. Draheim, and T. Tammet. Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia. In *Information Systems Frontiers*, 2023.

[92] S. Lips, N. Vinogradova, R. Krimmer, and D. Draheim. Re-shaping the EU digital identity framework. In *the 23rd Annual International Conference on Digital Government Research*, dg.o 2022, page 13–21, New York, NY, USA, 2022. Association for Computing Machinery.

[93] W. Lusoli, M. Bacigalupo, F. Lupiáñez-Villanueva, N. N. G. d. Andrade, S. Monteleone, and I. Maghiros. Pan-european survey of practices, attitudes and policy preferences as regards personal identity data management. *JRC Scientific and Policy Reports*, *EUR*, 25295, 2012.

[94] Z. Ma, R. Berglez, A. Bonitz, R. Kreissl, S. Vogl, L. Langer, and K. Srnec. A structured analysis of austrian digital identity for e-government services. In *CeDEM Asia 2014: Conference for E-Democracy an Open Government*, page 275, 2014.

[95] M. Maliappis, K. Gerakos, C. Costopoulou, and M. Ntaliani. Authenticated academic services through eidas. *International Journal of Electronic Governance*, 11(3-4):386–400, 2019.

[96] S. Mander, S. Lips, and D. Draheim. The utilization of public-private partnership frameworks in the management of eid projects. In *the 12th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2023. Springer, 2023.

[97] L. Marco, A. Pozo, G. Huecas, J. Quemada, and Á. Alonso. User-adapted web services by extending the eidas specification with functional attributes. *International Journal of Environmental Research and Public Health*, 18(8):3980, 2021.

[98] 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.

[99] M. Massoth. Mobile and user-friendly two-factor authentication for electronic government services using german electronic identity card and a nfc-enabled smartphone. *ICDS 2018*, page 10, 2018.

[100] 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].

[101] R. Medaglia, J. Hedman, and B. Eaton. Public-private collaboration in the emergence of a national electronic identification policy: The case of nemid in denmark. *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

[102] S. Mocanu, A. M. Chiriac, C. Popa, R. Dobrescu, and D. Saru. Identification and trust techniques compatible with eidas regulation. In *International Conference on Security and Privacy in New Computing Environments*, pages 656–665. Springer, 2019.

[103] F. Morgner, P. Bastian, and M. Fischlin. Attribute-based access control architectures with the eidas protocols. In *International Conference on Research in Security Standardisation*, pages 205–226. Springer, 2016.

[104] F. Morgner, P. Bastian, and M. Fischlin. Securing transactions with the eidas protocols. In *IFIP International Conference on Information Security Theory and Practice*, pages 3–18. Springer, 2016.

[105] A. Muldme, I. Pappel, M. Lauk, and D. Draheim. A survey on customer satisfaction in national electronic id user support. In *Proc. of ICEDEG 2018 – the 5th Intl. Conf. on eDemocracy & eGovernment*, pages 31–37. IEEE, 2018.

[106] N. Nan. Capturing bottom-up information technology use processes: A complex adaptive systems model. *MIS quarterly*, pages 505–532, 2011.

[107] O. Ngwenyama, H. Z. Henriksen, and D. Hardt. Public management challenges in the digital risk society: A critical analysis of the public debate on implementation of the danish nemid. *European Journal of Information Systems*, pages 1–19, 2021.

[108] P. of the United Kingdom. *Statutory Instrument No. 89 "The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019"*. Legislation.gov.uk, 2019.

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

[110] M. Oruaas and J. Willemson. Developing requirements for the new encryption mechanisms in the Estonian eID infrastructure. In *International Baltic Conference on Databases and Information Systems*, pages 13–20. Springer, 2020.

[111] T. J. Owens, D. T. Robinson, and L. Smith-Lovin. Three faces of identity. *Annual Review of Sociology*, 36:477–499, 2010.

[112] E. Palm and S. O. Hansson. The case for ethical technology assessment (eta). *Technological forecasting and social change*, 73(5):543–558, 2006.

[113] A. Parsovs. Solving the estonian id card crisis: the legal issues. In *ISCRAM 2020 Conference Proceedings-17th International Conference on Information Systems for Crisis Response and Management*, pages 459–471, 2020.

[114] A. Parsovs. Security improvements for the estonian id card. *Cybersec.ee*, 2022.

[115] K. Peffers, M. Rothenberger, T. Tuunanen, and R. Vaezi. Design science research evaluation. In K. Peffers, M. Rothenberger, and B. Kuechler, editors, *Design Science Research in Information Systems. Advances in Theory and Practice*, pages 398–410, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[116] R.-A. Petrauskas and P. Vaina. Development of electronic identification measures in the public sector in lithuania: reality, demand and the future. *Socialinės technologijos [elektroninis išteklius]*, pages 319–334, 2012.

[117] A. Poller, U. Waldmann, S. Vowé, and S. Türpe. Electronic identity cards for user authentication-promise and practice. *IEEE Security & Privacy Magazine*, 10(1):46–54, 2012.

[118] A. Preukschat and D. Reed. *Self-sovereign identity*. Manning Publications, 2021.

[119] J. Pries-Heje, R. Baskerville, and J. R. Venable. Strategies for design science research evaluation. *AIS Electronic Library (AISeL)*, 2008.

[120] T. Rissanen. Electronic identity in finland: Id cards vs. bank ids. *Identity in the Information Society*, 3(1):175–194, 2010.

[121] H. Roßnagel, J. Camenisch, L. Fritsch, T. Gross, D. Houdeau, D. Hühnlein, A. Lehmann, and J. Shamah. Futureid–shaping the future of electronic identity. *Datenschutz und Datensicherheit*, 36(3):189–194, 2012.

[122] S. Sädtler. Identity management in cloud computing in conformity with european union law?–problems and approaches pursuant to the proposal for a regulation by the european commission on electronic identification and trust services for electronic transactions in the internal market. *Open Identity Summit 2013*, 2013.

[123] M. S. H. A. Sallam, S. Lips, and D. Draheim. Success and success factors of the Estonian e-residency from the state and entrepreneur perspective. In *the 8th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2021, pages 291–304, Cham, 2022. Springer.

[124] J. Sánchez-García, J. M. García-Campos, D. Reina, S. Toral, and F. Barrero. Onsitedriverid: A secure authentication scheme based on spanish eid cards for vehicular ad hoc networks. *future generation computer systems*, 64:50–60, 2016.

[125] R. Saputro, I. Pappel, H. Vainsalu, S. Lips, and D. Draheim. Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study. In *the 7th International Conference on eDemocracy & eGovernment*, *ICEDEG 2020*, pages 216–222, 2020.

[126] S. Särav and T. Kerikmäe. E-residency: a cyberdream embodied in a digital identity card? In *The Future of Law and eTechnologies*, pages 57–79. Springer, 2016.

[127] C. Schmidt, R. Krimmer, and T. J Lampoltshammer. "when need becomes necessity"-the single digital gateway regulation and the once-only principle from a european point of view. *Open Identity Summit 2021*, 2021.

[128] J. Schot and A. Rip. The past and future of constructive technology assessment. *Technological forecasting and social change*, 54(2-3):251–268, 1997.

[129] S. Schwalm and I. Alamillo-Domingo. Self-sovereign-identity & eidas: a contradiction? challenges and chances of eidas 2.0. *Wirtschaftsinformatik*, 58:247–270, 2021.

[130] S. Schwalm, D. Albrecht, and I. Alamillo. eidas 2.0: Challenges, perspectives and proposals to avoid contradictions between eidas 2.0 and ssi. In H. Roßnagel, C. H. Schunck, and S. Mödersheim, editors, *Open Identity Summit 2022*, pages 63–74, Bonn, 2022. Gesellschaft für Informatik e.V.

[131] R. Sellung and H. Roßnagel. Evaluating complex identity management systems - the futureid approach. In D. Hühnlein, H. Roßnagel, R. Kuhlisch, and J. Ziesing, editors, *Open Identity Summit 2015*, pages 133–139, Bonn, 2015. Gesellschaft für Informatik e.V.

[132] A.-s. Shehu, A. Pinto, and M. E. Correia. On the interoperability of european national identity cards. In *International Symposium on Ambient Intelligence*, pages 338–348. Springer, 2018.

[133] H. A. Simon. *The Sciences of the Artificial, reissue of the third edition with a new introduction by John Laird*. MIT press, 2019.

[134] R. Smits and P. Den Hertog. Ta and the management of innovation in economy and society. *International Journal of Foresight and Innovation Policy*, 3(1):28–52, 2007.

[135] C. Sorge. The german electronic identity card: Lessons learned. In *Handbook of research on democratic strategies and citizen-centered E-Government services*, pages 214–230. IGI Global, 2015.

[136] D. Špaček. E-government policy and its implementation in the czech republic: Selected shortcomings. *Central European Journal of Public Policy*, 9(1):78–100, 2015.

[137] A. C. Stasis, L. Demiri, and E. Chaniotaki. eidas-electronic identification for cross border ehealth. *International Journal of Reliable and Quality E-Healthcare (IJRQEH)*, 7(2):51–67, 2018.

[138] H. Strack. Authentication and security integration for ecampus services at the university of applied sciences harz using the german electronic identity card/eid and egovernment standards. *Open Identity Summit 2013*, 2013.

[139] H. Strack, O. Otto, S. Klinner, and A. Schmidt. eidas eid & esignature based service accounts at university environments for cross boarder/domain access. *Open Identity Summit 2019*, 2019.

[140] H. Strack and S. Wefel. Challenging eid\& eidas at university management. *Lecture Notes in Informatics (LNI)*, 2016.

[141] H. Strack, S. Wefel, P. Molitor, M. Räckers, J. Becker, J. Dittmann, R. Altschaffel, J. Marx Gómez, N. Brehm, and A. Dieckmann. eid & eidas at university management-chances and changes for security & legally binding in cross boarder digitalization. In *Proceedings of the EUNIS 23rd Annual Congress, Münster, Germany*, pages 7–9, 2017.

[142] S. Stryker and P. J. Burke. The past, present, and future of an identity theory. *Social psychology quarterly*, pages 284–297, 2000.

[143] S. Stryker and R. T. Serpe. Identity salience and psychological centrality: Equivalent, overlapping, or complementary concepts? *Social psychology quarterly*, pages 16–35, 1994.

[144] C. Sullivan. Digital identity – from emergent legal concept to new reality. *Computer Law & Security Review*, 34(4):723–731, 2018.

[145] S. Sánchez García, A. Gómez Oliva, E. Pérez Belleboni, and I. Pau de la Cruz. Current trends in pan-european identity management systems. *IEEE Technology and Society Magazine*, 31(3):44–50, 2012.

[146] H. Tajfel. *Social identity and intergroup relations*, volume 7. Cambridge University Press, 2010.

[147] M. Talamo, S. Ramachandran, M.-L. Barchiesi, D. Merella, and C. Schunck. Towards a seamless digital europe: the ssedic recommendations on digital identity management. *Open Identity Summit 2014*, 2014.

[148] A. Tauber, T. Zefferer, and B. Zwattendorfer. Approaching the challenge of eid interoperability: An austrian perspective. *European Journal of ePractice*, 14:22–39, 2012.

[149] O. Terbu, S. Vogl, and S. Zehetbauer. One mobile id to secure physical and digital identity. In D. Hühnlein, H. Roßnagel, C. H. Schunck, and M. Talamo, editors, *Open Identity Summit 2016*, pages 43–54, Bonn, 2016. Gesellschaft für Informatik e.V.

[150] The Cooperation Network. *Opinion No. 1/2016 of the Cooperation Network on version 1.0 of the eIDAS Technical specifications*. The European Commission, 2016.

[151] The Cooperation Network. *Decision of the Cooperation Network on the need for open access to NFC interface to support secure mobile use of electronic identity means*. The Cooperation Network, 2019.

[152] The Cooperation Network. *Opinion No. 3/2019 of the Cooperation Network on the Dutch Trust Framework for Electronic Identification*. The CN, 2019.

[153] The Cooperation Network. *Opinion No. 4/2020 of the Cooperation Network on the Dutch eID scheme "DigiD"*. The CN, 2020.

[154] The Cooperation Network. *Guidance for the application of the levels of assurance which support the eIDAS Regulation*. European Commission, 2021.

[155] The Cooperation Network. *Opinion No. 2/2022 of the Cooperation Network on the new Czech eID means "MEG and MojeID"*. The CN, 2022.

[156] The Cooperation Network. *Opinion No. 4/2022 of the Cooperation Network on the changes in the Dutch eID scheme "DigiD"*. The CN, 2022.

[157] The Cooperation Network. *Opinion No. 5/2022 of the Cooperation Network on the Danish eID scheme "MitID"*. The CN, 2022.

[158] The European Commission. *Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance)*. Official Journal of the European Union, 2015.

[159] The European Commission. *Commission Implementing Desicion (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. Official Journal of the European Union, 2015.

[160] The European Commission. *Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*. Official Journal of the European Union, 2015.

[161] The European Commission. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. European Commission, 2019.

[162] The European Commission. *Inception Impact Assessment. Revision of the eIDAS Regulation - European Digital Identity (EUid)*. European Commission, 2020.

[163] The European Commission. *Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework*. European Commission, 2021.

[164] The European Commission. *Commissions staff working document "Impact Assessment Report" accompanying the document "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity"*. European Commission, 2021.

[165] The European Commission. *Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. European Commission, 2021.

[166] The European Parliament. *European Parliament resolution of 19 January 2016 on Towards a Digital Single Market Act (2015/2147(INI))*. Official Journal of the European Union, 2016.

[167] The European Union Agency for Cybersecurity. *Risk Management Standards. Analysis of Standardisation Requirements in Support of Cybersecurity Policy*. ENISA, 2022.

[168] T. Timan, A. F. van Veenstra, and K. Karanikolova. Measuring the impact of the once only principle for businesses across borders. In *The Once-Only Principle: The TOOP Project*, pages 208–224. Springer, 2021.

[169] M. Toots, T. Kalvet, and R. Krimmer. Success in evoting–success in edemocracy? the estonian paradox. In *International conference on electronic participation*, pages 55–66. Springer, 2016.

[170] N. Tsakalakis, S. Stalla-Bourdillon, and K. O'hara. What's in a name: the conflicting views of pseudonymisation under eidas and the general data protection regulation. *Open Identity Summit 2016*, 2016.

[171] N. Tsakalakis, S. Stalla-Bourdillon, and K. O'hara. Data protection by design for cross-border electronic identification: Does the eidas interoperability framework need to be modernised? In *IFIP International Summer School on Privacy and Identity Management*, pages 255–274. Springer, 2018.

[172] V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In *the 9th International Conference on Electronic Government and the Information Systems Perspective, EGOVIS 2020*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer.

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

[174] United Nations. Department of Economic and Social Affairs. *E-Government Survey 2022. The Future of Digital Government*. United Nations, New York, 2022.

[175] 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 *the 10th International Conference Electronic Government and the Information Systems Perspective, EGOVIS 2021*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer.

[176] J. van Dijck and B. Jacobs. Electronic identity services as sociotechnical and political-economic constructs. *New Media & Society*, 22(5):896–914, 2020.

[177] J. A. Vila, J. Serna-Olvera, L. Fernandez, M. Medina, and A. Sfakianakis. A professional view on ebanking authentication: Challenges and recommendations. In *2013 9th International Conference on Information Assurance and Security (IAS)*, pages 43–48. IEEE, 2013.

[178] E. Wagner, M. Mannino, and O. Lauer. Towards european electronic identity: A blueprint for a secure pan-european digital identity. *Journal of Financial Compliance*, 5(2):162–188, 2021.

[179] B. E. Whitley Jr and M. E. Kite. *Principles of research in behavioral science*. Routledge, 2012.

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

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

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

[183] M. Žagar, J. Knezović, B. Mihaljević, et al. Enabling reliable, interoperable and secure e-government services in croatia. *Central and Eastern European eDem and eGov Days*, 335:297–306, 2019.

[184] T. Zefferer and P. Teufl. Leveraging the adoption of mobile eid and e-signature solutions in europe. In *International Conference on Electronic Government and the Information Systems Perspective*, pages 86–100. Springer, 2015.

[185] T. Zefferer, D. Ziegler, and A. Reiter. Best of two worlds: Secure cloud federations meet eidas. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 396–401. IEEE, 2017.

[186] T. Zefferer, D. Ziegler, and A. Reiter. A federation of federations: Secure cloud federations meet european identity federations. *International Journal for Information Security Research*, 8(1), 2018.

[187] D. Zetzsche, D. Arner, R. Buckley, and R. Weber. The evolution and future of data-driven finance in the eu. *Common Market Law Review*, 57:331–360, 2020.

[188] B. Zwattendorfer and D. Slamanig. Design strategies for a privacy-friendly austrian eid system in the public cloud. *Computers & Security*, 52:178–193, 2015.

Acknowledgements

I want to thank and express my sincerest gratitude to my supervisor Dirk Draheim who has supported and encouraged me during my Ph.D. journey. Under your guidance, I have improved my academic skills and developed myself. I also would like to thank my co-supervisor Robert Krimmer for his motivating words, professional advice, and always calm attitude. I am incredibly grateful to my other co-supervisor Ingrid Pappel, who invited me to TalTech and encouraged me to start this journey.

I would also thank my employer State Information System Authority (RIA), for offering me an opportunity to be part of their expert team. I want to express my gratitude to my Cooperation Network colleagues, who have taught me so much. Thank you Helen, Herbert, Thorben, Noortje, Jiri, Felix, Mogens, Fredrik, Fabrice, Lucie and Romain. This work would not have been possible without RIA and my CN colleagues.

I am immensely thankful for my colleagues and co-PhD students with whom we have been publishing together, who have helped and supported me, and with whom I have had very exciting and fruitful discussions.

My warmest thanks go to my family, who has always been beside me throughout this journey. I am so glad I have inspired my kids and thankful for their understanding and supportive attitude. I know that I owe you my time.

Finally, I thank my friends and soulmates who have been beside me despite the weather.

Without your support and generosity, I would not have made it. I promise to continue to warrant your faith in me.

Thank you!

Silvia Lips
2023

Abstract
A Multifaceted Assessment Framework for Electronic Identity Schemes

For people living in Estonia, the use of e-services is an integral part of everyday life. However, communication and consumption of services at the level of the European Economic Area (EEA) with other countries is also becoming more and more important. There is also an increased interest in the use of Estonian e-services by EEA countries. In order to use the electronic identity (eID) tools of different countriesacross the borders in the EEA, each country must notify its eID scheme for cross-border use according to the European Union regulation on trust services required for e-identification and e-transactions in the internal market (eIDAS). The eID scheme can be notified at levels of 'low', 'substantial' and 'high'. Unfortunately, the existing notification procedure is complex and time-consuming, and it is difficult to compare eID schemes notified at the same level. Based on the above, the aim of this doctoral thesis is to propose a framework that enables the assessment of the eID schemes of different countries and their levels more easily and objectively. For this purpose, the author analyzes the eIDAS regulation implementation practice in Estonia as well as in other European countries and conducted structured in-depth interviews with eID experts from 9 countries who participated in the eID schemes assessment process. The research follows the design science research methodology and relies on three theoretical foundations (institutional design by Koppenjan and Groenewegen, identity theory and technology assessment theory). The multifaceted assessment framework for eID schemes (eIDAF) created as a result of the research includes innovations at the process level, in the documentation and in the assessment principles.

Kokkuvõte
Elektrooniliste autentimisskeemide mitmetahuline hindamise raamistik

Eestis elavate inimeste jaoks on e-teenuste kasutamine igapäevaelu lahutamatuks osaks. Kuid üha olulisemaks muutub ka suhtlemine ja teenuste tarbimine Euroopa Majandusühenduse (EMÜ) tasandil teiste riikidega. Samuti on EMÜ riikide poolt suurenenud huvi Eesti e-teenuste kasutamiseks. Selleks, et erinevate riikide elektroonilise identiteedi (eID) vahendeid oleks võimalik EMÜ-s piiriüleselt kasutada, peab iga riik Euroopa Liidu määrusest e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul (eIDAS) tulenevalt oma eID skeemi piiriüleseks kasutamiseks teavitama. eID skeemi saab teavitada tasemel „madal“, „märkimisväärne“ ja „kõrge“. Paraku on olemasolev teavitamise protseduur keerukas ja aeganõudev ning samal tasemel teavitatud eID skeeme keeruline võrrelda. Eeltoodust tulenevalt on käesoleva doktoritöö eesmärgiks välja pakkuda raamistik, mis võimaldaks erinevate riikide eID skeeme ja nende tasemeid lihtsamalt ja objektiivsemalt hinnata. Selleks analüüsib autor nii Eesti kui ka teiste Euroopa riikide eIDAS määruse rakendamise praktikat ning viib läbi struktureeritud süvaintervjuud 9 riigi eID valdkonna ekspertidega, kes osalevad eID skeemide hindamise protsessis. Teadustöö järgib design science uurimismetoodikat ning toetub kolmele teoreetilisele alusele (Koppenjani ja Groenewegen-i institutsionaalne disain, identiteedi teooria ning tehnoloogia hindamise teooria). Uurimistöö tulemusena valminud eID skeemide hindamise raamistik (eIDAF) hõlmab uuendusi protsesside tasandil, esitatavas dokumentatsioonis ja teabes ning hindamise põhimõtetes.

Appendix 1

I

S. Lips, V. Tsap, N. Bharosa, R. Krimmer, D. Draheim, and T. Tammet. Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia. In *Information Systems Frontiers*, 2023

Management of National eID Infrastructure as a State-Critical Asset and Public-Private Partnership: Learning from the Case of Estonia

Silvia Lips[1*], Valentyna Tsap[2], Nitesh Bharosa[3], Robert Krimmer[4], Tanel Tammet[5] and Dirk Draheim[1*]

[1]Information Systems Group, Tallinn University of Technology, Akadeemia tee 15a, Tallinn, 12169, Estonia.

[2]Cybernetica AS, Mäealuse 2/1, Tallinn, 12618, Estonia.

[3]Department of Engineering Systems & Services, Delft University of Technology, Jaffalaan 5, Delft, 2628 BX, the Netherlands.

[4]Johan Skytte Institute of Political Studies, University of Tartu, Lossi 36, Tartu, 51003 Estonia.

[5]Applied Artificial Intelligence Group, Tallinn University of Technology, Akadeemia tee 15a, Tallinn, 12169, Estonia.

*Corresponding author(s). E-mail(s): silvia.lips@taltech.ee; dirk.draheim@taltech.ee;
Contributing authors: valentyna.tsap@cyber.ee; n.bharosa@tudelft.nl;
robert.krimmer@ut.ee; tanel.tammet@taltech.ee;

Abstract

In the management of national electronic identity (eID) infrastructure, cooperation between public and private parties becomes more and more important, as the mutual dependencies between the provision of e-services and the provision of the national public key infrastructure (PKI) continuously increases. Yet, it is not clear which key factors affect the public-private collaboration in the eID field, as existing studies do not provide insight into this particular matter. Therefore, we aim to identify the factors that affect public-private partnership (PPP) in the field of eID. We also describe feasible formats that help to improve the cooperation between the two sectors, based on insights from the case of Estonia. In service of that study, we conducted twelve qualitative interviews with high-level experts representing several parties from the public and the private sector. By conducting a thematic analysis of the interviews, we identified five key factors for successful PPP in the eID field, i.e., engagement, joint understanding, two-way communication, clear role division, and process orientation. Furthermore, we generalize our results by discussing, in how far the found cooperation formats can be used by stakeholders to manage state-critical information technology (IT) infrastructure components similar to eID such as mobile phone services, data transmission services and digital signature services.

Keywords: electronic identity, identity management, public-private partnership, critical infrastructure management

1 Introduction

Digital technology and e-services play an increasingly critical role in today's society. For example, try to imagine a situation where doctors are not able to log in to their databases to look up their patients' health information, so that it becomes impossible to issue prescriptions. In this situation it is hard to provide emergency help. This is exactly what happened in 2017, when Estonia faced a security vulnerability on electronic identity (eID) cards, that has become known as the so-called Return of the Coppersmith Attack (ROCA). Quickly, it became clear that the existing public key infrastructure (PKI) infrastructure plays a critical role at national scale. The vulnerability itself affected approximately 800,000 eID cards and was solved in cooperation with public and private sector stakeholders (Lips et al, 2018; Valtna-Dvořák et al, 2021).

Public-private partnership (PPP) is common in the development and maintenance of nationally important infrastructure components (Sehgal and Dubey, 2019). Well-known examples of critical infrastructure are energy supply, transportation, food supply, water supply, healthcare (Filiol and Gallais, 2014), financial systems, civil administration, transportation systems, chemical industry (Alcaraz and Zeadally, 2015), and – last but not least – information and communications technologies (ICT). At the level of the European Union, the European Commission takes actions to protect critical European infrastructures and has launched the European Program for Critical Infrastructure Protection (EPCIP) (Pursiainen, 2018). Despite of that, every country defines more specifically, which areas are part of the critical infrastructure and how they are managed. For example, e-governance related services such as authentication and digital signing were recently considered as a part of state-critical infrastructure in Estonia (Tsap et al, 2020b). The Estonian Emergency Act[1] states that, starting from 2018, digital identification and digital signing (more generally expressed as electronic eID ecosystem) are parts of the Estonian state-critical infrastructure. The Estonian eID ecosystem includes various public and private sector stakeholders. Their cooperation capability and their maturity of managing state-critical infrastructure become significant in terms of PPP.

To understand the correlations between the stakeholders and their mutual impact in the critical infrastructure management, we aim to answer the following research questions:

- *RQ1.* Which factors affect the public-private cooperation in the field of eID?
- *RQ2.* How to improve the public-private cooperation in the field of eID?

We use triangulation to answer the research questions – we have interviewed 12 experts from the public and the private sector, have conducted a thematic analysis of these interviews, provide a detailed overview of the Estonian eID ecosystem and analyse other studies focusing on factors affecting critical infrastructure management. Moreover, we analyze several alternative cooperation formats in the field of eID.

The research topic is complex and consists of various layers. Therefore, we use the institutional design framework for complex technological systems proposed by Koppenjan and Groenewegen (2005) as a theoretical background to analyze and describe the eID infrastructure, stakeholders and relations through several institutional layers.

This paper is organized as follows. In Sect. 2, we provide a brief overview of existing work as well as necessary background information regarding Estonian eID stakeholders, their roles and responsibilities in managing parts of the eID state-critical infrastructure. Section 2 helps to understand the background and its relation to the theoretical concepts creating the overall framework for the research. In Sect. 3, we present the qualitative research approach of this paper, which is embedded in the context of a larger action design research (ADR) (Sein et al, 2011) project. In Sect. 4, we present the main research findings including the factors that affect the cooperation in the eID field, together with alternative cooperation formats proposed by the interviewees, and discuss the research findings in a wider context. Finally, In Sect. 5, we provide a conclusion including an overview of research limitations and possible future research directions.

[1] https://www.riigiteataja.ee/en/eli/525062018014/consolide

2 Setting the Scene

In this section, we provide a more detailed overview of existing works on factors affecting PPP from several perspectives. On the basis of the theoretical analysis framework proposed by Koppenjan and Groenewegen (2005), we describe the Estonian identity management ecosystem, identify relevant stakeholders and explain their roles.

2.1 Literature Review

2.1.1 PPP and Critical Infrastructure Related Studies

PPP is a well-researched topic in its own right. It is possible to find a series of PPP-related research papers from various perspectives such as the financier's perspective (Owolabi et al, 2020), the front-line employee's perspective (Tawalare et al, 2020; Tsap et al, 2020a) and the public partner's perspective (Ghribi et al, 2019). Some research papers remain more at a theoretical level, while others are practice-oriented and focus on a certain industry such as construction (Li et al, 2005), water infrastructure (Dithebe et al, 2019) and healthcare (Wróbel, 2019). An example of a more theoretical study is (Das Aundhe and Narasimhan, 2016), that analyzes how and why the intangible factors influence PPP outcomes. An example for a study at a rather practical level is (Paide et al, 2018a), that investigates how to strengthen the collaboration between the Estonian public and private sector through improvement of Estonia's nation-wide data exchange platform X-Road. There has been also research on PPP in the eID field focusing on factors that influence the distribution of power between public and private sector authorities (Medaglia et al, 2017). Medaglia et al (2017) use the power dependence theory to analyse the eID tender process in Denmark.

Several research papers focus on PPP in projects related to critical infrastructure in developing countries (Debela, 2019; Alinaitwe and Ayesiga, 2013; Ayo-Vaughan et al, 2019; Osei-Kyei and Chan, 2019). Debela (2019) focuses on the PPP success factors in the Ethiopian road sector. Alinaitwe and Ayesiga (2013) analyse PPP in the construction industry in Uganda and Ayo-Vaughan et al (2019) identifies PPP success factors in the aviation sector in Nigeria. Hai et al (2022) identify PPP success factors in infrastructure projects in Vietnam.

PPP cooperation is often utlized in protection of critical infrastructure, however, not always the most efficient way. Dunn-Cavelty and Suter (2009) analyse positive aspects and limitations of PPP in critical infrastructure protection and suggests a network-oriented approach based on governance theory Schuppert (2015) as an alternative way of cooperation.

Despite of various studies on different aspects of PPP, it still lacks a systematic understanding of PPP from the eID perspective, i.e., which factors influence the cooperation between the two sectors and what could be alternative collaboration formats. Moreover, combining the fields of eID and critical infrastructure leads to further interesting research questions that we would like to address.

2.1.2 Factors Affecting PPP Projects

Based on the literature, there are two types of PPP studies, i.e., dealing with success factors analysis (Dithebe et al, 2019), on the one hand, and dealing with risk factor analysis (Ghribi et al, 2019), on the other hand. Moreover, Mulyani (2021) has carried out a general analysis of articles focusing on PPP success factors. Even though it is important to pay attention to risk factor analysis, the current paper focuses on success factors influencing PPP.

Section 2.1.2 focuses on studies conducted during the last ten years. Osei-Kyei and Chan (2015) conducted a review of studies on critical success factors of PPP projects from 1990 to 2013, and according to this study, the most common factors are "risk allocation, risk sharing, strong private consortium, support at the level of politics, community and citizens and transparent procurement" (Osei-Kyei and Chan, 2015). Factors vary depending on the industry (water, construction etc.). Tang et al (2010) has conducted a review of PPP studies in the construction industry. Węgrzyn et al (2016) focuses on the critical success factors for PPP in different stakeholder groups, stating that stakeholder role in the project plays significant role in the project success. Table 1 gives a detailed overview of the PPP success factors identified from the literature.

Publication	Research Focus	Factors
Osei-Kyei and Chan (2015)	General study	"Risk allocation and sharing, strong private consortium, political support, community/public support and transparent procurement."
Jacobson and Ok (2008)	General study	"Specific plan/vision, commitment, open communication and trust, willingness to compromise/collaborate, respect, community outreach, political support, expert advice and review, risk awareness, and clear roles and responsibilities."
Babatunde et al (2016)	PPP projects in Nigeria	"Reliable concession arrangement with due diligence; serious commitment with adequate technical strength; favourable economic environment; government support with enabling legislation; bankable project with adequate stakeholders involvement; and strong "political will" with committed private partners."
Sanni (2016)	PPP projects in Nigeria	"Projects feedback, leadership focus, risk allocation and economic policy, good governance and political support, short construction period, favourable socio-economic factors, and delivering publicly needed service."
Hsueh and Chang (2017)	PPP projects in Taiwan	"Supportive legal frameworks, a favorable investment environment, selection of appropriate PPP projects and public support."
Chan et al (2010)	PPP projects in China (infrastructure)	"Stable macroeconomic environment, shared responsibility between public and private sectors, transparent and efficient procurement process, political and social environment, judicious government control."
Ismail (2013)	PPP projects in Malaysia	"Good governance", "commitment of the public and private sectors", "favourable legal framework", "sound economic policy" and "availability of finance market".
Muhammad and Johar (2018)	PPP projects in Malaysia and Nigeria (housing)	Nigeria ('equitable risk allocation', 'stable political system', and 'reputable developer'). Malaysia ('action against errant developer', 'consistent monitoring', and 'house buyer's demand').
Li et al (2005)	PPP projects in UK (construction)	"Effective procurement, project implementability, government guarantee, favourable economic conditions and available financial market."
Surachman et al (2020)	PPP projects in Indonesia (water)	"Support and acceptance of the stakeholders from the community, whereas the private and public entities are the second and third important factors."
Dithebe et al (2019)	PPP in water supply projects	"Thorough planning for project viability, high levels of transparency and accountability and a legal framework stipulating policy continuity."
Ameyaw and P.C. Chan (2016)	PPP in water supply projects	"Commitment of partners, strength of consortium, asset quality and social support, political environment, and national PPP unit."

Table 1 Factors affecting PPP according to the literature

Various studies analyze the implementation of several types of PPP in infrastructure development projects in developed and developing countries (Zhang, 2005; Babatunde et al, 2016; Hsueh and Chang, 2017; Chan et al, 2010; Ismail, 2013; Li et al, 2005; Firmino, 2018). Dithebe et al (2019) argue that critical success factors for water infrastructure projects conducted under PPP are "public cooperation, project viability and policy and legislation enhancement" (Dithebe et al, 2019). Li et al (2005) have conducted research on construction projects in the United Kingdom, which shows that critical success factors for PPP are "a strong and good private consortium, appropriate risk allocation and available financial market" (Li et al, 2005). Jacobson and Ok (2008) conducted a general study about PPP and public works in which they define ten success factors that affect the collaboration: "specific plan/vision, commitment, open communication and trust, willingness to compromise/collaborate, respect, community outreach, political support, expert advice and review, risk awareness, and clear roles and responsibilities" (Jacobson and Ok, 2008). Sehgal and Dubey (2019) studied PPP project success factors in the literature and identified fourteen significant components including "long lasting macroeconomic environment, mutual understanding between two sectors, ethical and expeditious procurement process, socio-political aspects, government involvement and interference, relationship management, institutional factors, project planning" (Sehgal and Dubey, 2019). Ismail (2013) conducted a case study of Malaysia and identified five main success factors, i.e. "«good governance», «commitment of the public and private sectors», «favorable legal framework», «sound economic policy» and «availability of finance market»" (Ismail, 2013).

A lot of studies identify PPP success factors in developing countries (Ameyaw and P.C. Chan, 2016; Babatunde et al, 2016; Muhammad and Johar, 2018; Surachman et al, 2020). One of these examples is the study by Babatunde et al (2012) about PPP in delivering infrastructure in Nigeria, which showed that public and private sector views on critical success factors is different. In a later study from Nigeria from 2016, Sanni (2016) determined seven critical factors affecting PPP projects: "feedback, leadership focus, risk allocation and economic policy, good governance and political support, short construction period, favorable socio-economic factors, and delivering publicly needed service" (Sanni, 2016). Alinaitwe and Ayesiga (2013) investigated the case of construction industry in Uganda and found that success factors are "competitive procurement process, a well-organised private sector, the availability of competent personnel to participate in PPP project implementation, and good governance" (Alinaitwe and Ayesiga, 2013).

While conducting the literature review, we did not find similar works carried out directly in the field of eID, not even in the field of ICT (information communication technology). Papers mainly focus either on large-scale infrastructure projects such as water management, energy supply, aviation sector or on case studies of developing countries (Ameyaw and P.C. Chan, 2016; Babatunde et al, 2016; Muhammad and Johar, 2018; Surachman et al, 2020), or comparison of several practices such as the study of Cheung et al (2012b).

Moreover, it is noticeable that there is no common list of success factors. At a general level, it is possible to find some similar factors such as cooperation, collaboration and political aspects irrespective of the geographical locations Cheung et al (2012a); however, it is not sufficient to say that there is a clear list of uniform factors affecting successful cooperation in case of PPP.

2.2 Estonian Identity Management

2.2.1 The Level of Digitalization in Estonia

The level of digitalization in Estonia is particularly high. For example, the two most recent UN e-Government Surveys 2018 and 2020 (UN Department of Economic and Social Affairs, 2018, 2020) clearly describe Estonia as a technological leader. In the 2018 survey, the case of Estonia defines the e-government category "Government as an API" (Application Programming Interface). Then, the survey 2020 concludes that "Estonia is considered one of the fastest raising countries for digital transformation in the world." (UN Department of Economic and Social Affairs, 2020). And indeed, Estonia has clearly identifiable digital assets. Most of the state services are accessible online. 98% of the Estonian population have an

ID-card containing a chip that enables digital authentication and digital signing; and about 2/3 of the eID owners use it regularly.[2]

The "Government as an API" is the key to this success story. The foundation of this approach is Estonia's data exchange layer X-Road (Ansper, 2001; Kalja, 2008, 2012; Willemson and Ansper, 2008; Ansper et al, 2013; Kalja et al, 2015; Paide et al, 2018b; Saputro et al, 2020)[3,4,5,6]. The Estonian regulation on X-Road (Regulation no. 105, 2016) defines that "the data exchange layer of information systems (hereinafter X-Road) is a technical infrastructure and instance between the members of X-Road, which enables secure online data exchange, ensuring evidential value".

X-Road is a peer-to-peer data exchange system teaming together

- a PKI (public key infrastructure),
- sophisticated software components for secure data exchange,
- a nomenclature of metadata items associated with each message along the core representation language and structure of messages,
- systematic (regulated Regulation no. 105 (2016)) organizational measures.

A key to successful architecture of digital government ecosystems is in understanding data governance, which aims at the following data principles: (i) data protection (European Commission, 2016), (ii) data quality (Tepandi et al, 2017; Draheim and Nathschläger, 2008), and (iii) the once-only-principle (Kalvet et al, 2018). In the context of digital government, data governance is an ultra large-scale, cross-organizational challenge. Based on experience and analysis of the Estonian e-government ecosystem, we have elaborated a digital government architecture framework based on the following line of hypotheses, see (Draheim et al, 2021; Draheim, 2021):

- The form of state's institutions follows the state's functions. The entirety of the state's institutions (i.e., their shape, their interplay) makes the state's *institutional architecture*. The institutional architecture changes slowly.
- The state's institutional architecture determines the state's *data governance architecture*. The data governance architecture links data assets with accountable organizations.
- The data governance architecture limits the design space of the *digital government solution architecture*, which consists of all *digital administrative processes* and delivered *e-services*. The digital government solution architecture can show small, ad-hoc and fast changes.
- Changes in the institutional architecture are so severe that they can trigger immediate changes in the digital government solution architecture, whereas changes in the digital government solution architecture can only have a long-term influence on changes in the institutional architecture.

We say that the data governance architecture and the digital government solutions architecture together form the *digital government architecture*. The data governance architecture forms the backbone, that deals with the necessary fulfilment of data governance; whereas the solutions architecture addresses all kinds of quality aspects of the offered solutions, i.e., usefulness, adherence to good service-design principles, maturity of processes etc.

2.2.2 Estonian Identity Management Stakeholders

According to the Estonian Information System Authority, public and private entities offer, in total, more than 5000 e-services (E-Governance Academy, 2016). In practice, this means that many critical sectors such as healthcare and the internal security sector depend on PKI-based (public key infrastructure) e-governance services. Any kind of deviations from usual operation and availability of the services can cause at least inconvenience and excessive confusion and chaos in the worst case.

Before it is possible to analyze factors influencing PPP, it is important to provide an overview of the most important players in the Estonian identity management system (IMS). Figure 1 shows the stakeholders' perspective, including relations between different stakeholders and their main roles. It is important to note that, due to the high number of players, the service provider's

[2] https://e-estonia.com/solutions/e-identity/id-card/

[3] X-tee in Estonian; in English: originally pronounced as 'crossroad', nowadays pronounced as 'x road'

[4] https://x-road.global/

[5] https://www.niis.org/

[6] https://x-road.global/

perspective is not included in Fig. 1. The perspective of ministries and policy makers are not shown in Fig. 1. They are part of the IMS but not directly involved with the eID scheme. In its center, Fig. 1 shows the several public sector eID tokens (smart-card- or SIM-card-based solutions) that are currently in use to enable digital authentication and digital signing.

The degree of involvement of the private sector in the IMS is remarkably high throughout the whole process, starting from eID manufacturing, personalization, over generation of certificates to the final delivery to the end-user. Telecommunication companies issue mobile-IDs and, it is possible to receive e-residency digital identity cards from external service provider offices in various foreign countries. In this example, it is fair to say that public and private sector activities intertwine well and relations between the parties play a significant role in the service delivery process.

Furthermore, the Estonian eID ecosystem involves many parties and roles from the public and private sector that are indirectly involved with the IMS. In Table 2 and Table 3, we provide a detailed overview of the authorities and their roles in the IMS.

A more detailed overview of the Estonian IMS is provided by the State Information System Authority's blog.[7]

3 Research Methodology

In 2018, the Estonian Police and Border Guard Board (PBGB) and the Estonian Information System Authority (RIA) initiated a process to create an identity management strategy. As a result of this process, eID stakeholders from the public and the private sector proposed a strategic white paper on identity management and identity documents (IMID).[8] Lips et al (2019) provide an overview of the strategic planning process in the critical infrastructure management based on ADR (Action Design Research) principles (Petersson and Lundberg, 2016).

This paper presents a concrete case study of the IMID strategic planning process. The focus of this case study research (Yin, 2011) is on in-depth analysis of qualitative data collected in regard to critical infrastructure management.

As a theoretical foundation, we use institutional design framework for complex technological systems proposed by Koppenjan and Groenewegen (2005), since it allows for understanding complex and multi-layered systems such as an eID ecosystem more systematically. The framework of Koppenjan and Groenewegen (2005) adapts Williamson's four-layer analysis model of institutional economics (Williamson, 1979, 1998). Bharosa et al (2020) argue that the model of Koppenjan and Groenewegen (2005) is particularly well suited for the analysis of e-government systems. Table 4 describes the Estonian eID ecosystem through the four institutional layers of (Koppenjan and Groenewegen, 2005).

To answer our research questions, we interviewed half of the experts who participated in the IMID development process. In total, we conducted twelve interviews: five with experts from the public sector and seven with experts form the private sector. We selected the interviewees according to their role in the eID scheme. The aim was to cover the public and private sectors' views from different angles (token production, personalization, certificate issuance, certificate management, identity document issuance, policy making, e-service provision etc.). Table 5 provides a detailed overview of the interviewees and their roles.

The interviews were individual, semi-structured, and non-standardized and consisted of eight questions. Some questions consisted of two to three sub-questions. We conducted the interviews mostly in the location of the interviewees and in Estonian. One interview was conducted online in English. We recorded all interviews based on interviewees' prior consent. Interviewees were informed and aware about the purpose of the research and the interviewees gave their consent to use their answers also for further research purposes.

We transcribed all interviews, coded the transcriptions and conducted a thematic analysis of the data (Vaismoradi et al, 2013) to identify the critical success factors that influence PPP. Figure 2 illustrates the data validation process in detail (Creswell, 2014).

[7] https://blog.ria.ee/2018/05/

[8] https://www.ria.ee/sites/default/files/content-editors/EID/valge-raamat-2018.pdf

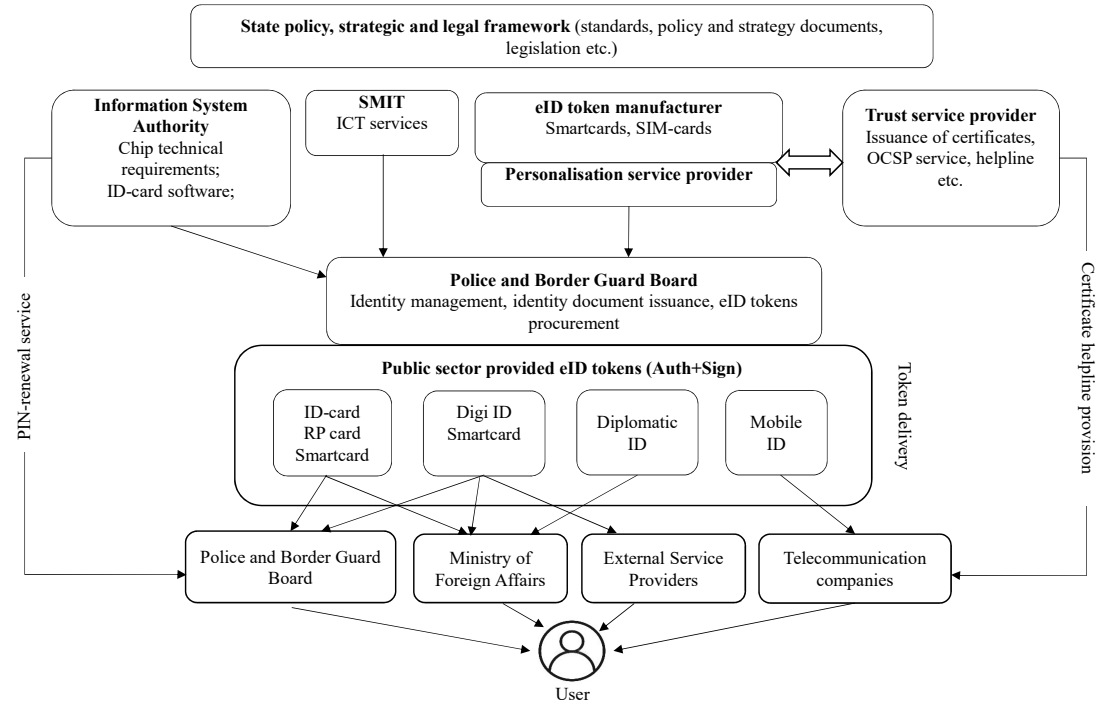

Fig. 1 The Estonian eID scheme from a stakeholders' perspective.

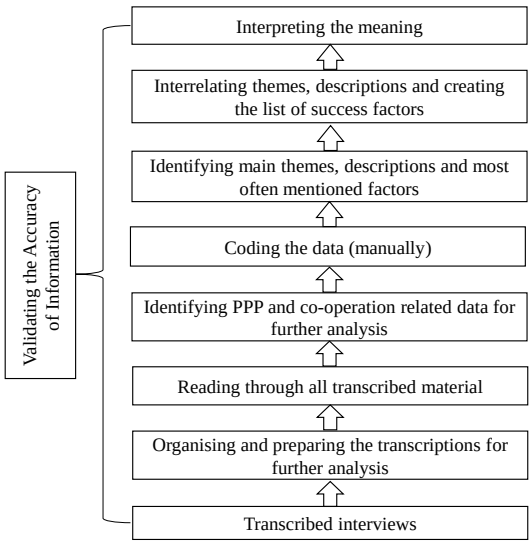

Fig. 2 Data analysis model

4 Research Results and Discussion

It is important to point out that during the IMID development the focus was rather on the strategic, long-term cooperation between the public and the private sector than on everyday collaboration. We distinguished daily cooperation solving individual issues from long-term future-oriented cooperation, because both forms of cooperation require different collaboration formats. However, many of the prerequisites and characteristics are general and may apply in both cases. The Estonian IMS is a good example of strategical cooperation between the public and the private sector and, therefore, offers a good opportunity to analyse existing shortcomings and to identify areas that need improvement.

During the data analysis process, we identified three main themes and one sub theme:

1. Existing cooperation evaluation;
2. Stakeholder environment analysis;
3. Proposals to improve the situation;

Public Sector Stakeholders	Responsibility
Police and Border Guard Board (PBGB)	Accordig to the Regulation no. 33 (2014) PBGB is responsible for identification of persons and identity management. PBGB procures identity document tokens and ensures their issuance. Furthermore, PBGB is responsible for the Estonian eID scheme description for cross-border usage.
Estonian Information System Authority (ISA)	According to the Regulation no. 28 (2011) ISA is responsible for eID software and for the development and management of the trust services infrastructure. The authority is also responsible for national cybersecurity incidents handling and has a supervisory role over the trust service providers.
IT and development center of the Ministry of the Interior of Estonia (SMIT)	According to the Regulation no. 8 (2020) SMIT develops, procures and manages ICT systems in the area of internal security, including information systems related to identity management and identity documents.
Ministry of the Interior (SiM)	According to the Regulation no. 39 (2012) SiM is responsible for shaping the identity management and the identity documents issuance policy.
Ministry of Economic Affairs and Communications (MKM)	According to the Regulation no. 323 (2002) MKM is responsible for shaping and coordinating the Estonian information society policy.
Ministry of Foreign Affairs (MFA)	According to the Regulation no. 196 (2004) MFA ensures the protection of interests of Estonians in foreign countries. Receives identity document applications and issues identity documents
Enterprise Estonia	Responsible for the e-residency program; creates pre-conditions for the development of e-services.

Table 2 IMS (identity management system) stakeholders from the Estonian public sector and their roles.

Private Sector Stakeholders	Responsibility
Trust service provider (SK ID Solutions AS)	Responsible for issuing the certificates for the Estonian identity documents and provider of related services.
ID manufacturer (IDEMIA France S.A.S)	Responsible for manufacturing blank identity documents.
Personalization service provider (Hansab AS)	Responsible for personalization of identity documents.
Banks	Provided the PIN replacement service until 28.02.2019.
Telecommunication service providers	Responsible for issuing SIM-cards with mobile-ID capacity.
External service providers (VFS Global)	Responsible for offering eResidency issuance service (including identification).

Table 3 Estonian IMS private sector stakeholders and their roles.

(a) Alternative cooperation formats.

Under the first theme, we identify issues that affect the current cooperation negatively. The second theme focuses on stakeholders' involvement analysis. Finally, we map all cooperation related proposals from the interviewees and provide generalized conclusions that other countries can consider when developing their national eID schemes and defining critical infrastructure components.

Due to the complexity of the topic, we decided that it is not reasonable to artificially separate the presentation of the research results from their discussion. We present our findings according to

Layer	Estonian eID Ecosystem
Layer 4: Informal institutional environment	People trust the government. Public sector institutions are responsible for the eID ecosystem and provision of e-services (Muldme et al, 2018). Public and private institutions develop the eID area in close cooperation and set strategical goals together (Lips et al, 2019).
Layer 3: Formal institutional environment	The Estonian eID ecosystem relies on the EU eIDAS (electronic identification and trust services for electronic transactions in the internal market) regulation. At the national level, two main legal acts are regulating the eID ecosystem: Electronic Identification and Trust Services for Electronic Transactions Act and Identity Documents Act.
Layer 2: Formal and informal institutional arrangements	Identity documents strategy proposed by public and private sector experts (Lips et al, 2019). Regular meetings between public and private sector representatives organized by Information Systems Authority. Estonian Police and Boarder Guard Board and IDEMIA S.A.S. have concluded a contract for the production of eID cards.
Layer 1: Actors and games	A detailed overview over the Estonian eID ecosystem actors and dependencies between the stakeholders is presented in Fig. 1, Table 2 and Table 3.

Table 4 Estonian eID ecosystem analysis based on the model of Koppenjan and Groenewegen (2005).

the three main themes (and one sub-theme) and interpret the results.

4.1 Evaluation of Established Cooperation

During the IMID development process, it has become clear that the question is not only about selecting the best strategical choices for the country but also about starting substantive discussions between public and private sector eID stakeholders. To provide a holistic overview of the research results, we present positive and negative aspects that, according to the interviewees, affect the collaboration between the two sectors in Table 6 .

In general, the interviewees perceived as positive that the public sector initiated a strategic discussion on identity management and identity documents and that several different stakeholders have been asked for their opinion. Furthermore, the interviewees liked the moderated workshop format. The fact that experts from both sectors knew each other well from their previous positions and that the circle of experts was limited had both positive and negative impact.

However, more than half of the interviewees admitted that the cooperation between the public and the private sector needs improvement. Most common aspects (three or more interviewees named it) were: negative attitude, negative preconception, lack of involvement and shortcomings in the feedback process.

Eight interviewees mentioned that they sensed a negative attitude from one or another side during the collaboration. Interviewees brought out keywords such as offence, conflict, dissension, negative preconception, pessimism, and dispute. Two interviewees said that more than 10 years ago the cooperation was at a much better level. According to one interviewee, in 2001, when first Estonian digital identity card was launched, the cooperation between the public and the private sector was very good and productive, whereas currently, there exists almost no cooperation, it lacks a feeling of unity, and public and private sector experts need to rebuild the cooperation again. Another interviewee said that strategical documents neither solve problems nor provide solutions. Therefore, it is important to invest into community building and to have strong lobbying groups. Five interviewees did not mention either of the sectors as specific in regard to negative attitude. Two interviewees found that the negative attitude is more on the public sector side and one interviewee found that it is more on the private sector side. Four interviewees did not mention negative attitude as an issue.

Organization name	Role	Interest/Focus	Category
Police and Border Guard Board	Head of Identity and Status Bureau	User friendliness / UX of e-services (authentication, digital signing)	Public
State Information System Authority	Head of an eID branch	Engagement of the state in the eID field and long-term perspective.	Public
SK ID Solutions AS	CEO	Ensuring that the process outcome is comprehensive.	Private
Ministry of the Interior	Adviser	Identity management policy (especially identity documents issuance).	Public
Cybernetica AS	Member of the Supervisory Board	Security of the electronic identity systems.	Private
Estonian Association of Information Technology and Telecommunications (ITL)	Vice-President (digital infrastructure)/Chairman of the Board (AS Levira)	Community level agreement about secure devices that public and private sector uses and promotes.	Private
ITL	CEO	Long-term view of the whole area.	Private
ITL	Software Development and Technology Director (AS Datel)	Business architecture.	Private
Estonian Banking Association	Head of Digital Strategy in Baltic Division at SEB Bank	Evolvement of digital identity and services built on it.	Private
Police and Border Guard Board	Adviser-Expert	Identity management.	Public
IDEMIA	Head of Citizen Markets	Security and user experience.	Private
IT and Development Center (Ministry of Interior)	Product owner	Procedural matters related to identity documents.	Public

Table 5 Interview participants and their roles.

Positive aspects	Negative aspects
• Joint meetings with a strategic focus • Workshops initiated by the public sector • Public and private sector experts know each other from previous positions	• Negative attitude and prejudices • Poor involvement in discussions • Lack of feedback for proposals • Exclusion of important stakeholders • Unclear processes • Lack of interest • Limited time to contribute • Different perceptions and understandings • Unclear responsibility and role division • Subjectivity • Complex regulatory environment

Table 6 Positive versus negative aspects of the collaboration.

Before involving the private sector, the public sector tried to shape its own position and had several meetings regarding the IMS. Some private sector representatives found that they were not involved in important discussions from the beginning; and even in cases where they were involved, they did not receive sufficient feedback to their proposals.

A couple of interviewees pointed out that some important stakeholders were missing and that the strategy building process was unclear. Some interviewees mentioned that some of the public sector representatives did not show enough interest during the meetings and that they just attended for having attended. One interviewee admitted that he wanted to contribute more but due to other tasks, the time was limited.

One interesting finding was that public and private sector representatives had different perceptions and understandings already at the level of basic terminology. Experts talked about the same topic but used different semantics. Sometimes, it took some time before the experts realized that their positions were actually not contradictory.

Interviewees from the private sector pointed out that the division of roles in the field of electronic identity is not clear enough. Several authorities and even ministries are responsible for the same area at the same time. Main themes are clear but when it comes to specific questions, there are lot of grey areas and ambiguities.

Subjectivity is another factor that has been mentioned by interviewees various contexts. For example, one interviewee said that subjectivity at the level of policy making limits possible developments and available alternatives. Another interviewee found that the circle of eID experts is very limited, i.e., consisting of people who have worked in the public sector first and than in the private sector or vice versa. On the one hand, this can simplify the communication between the parties; but it was also a barrier in the past, whenever the cooperation was not smooth .

Finally, the interviewees found that the whole eID ecosystem has become more complex – not only from the technical perspective and with respect to role division, but also in regard to policy and the legal environment. Since 2001, the legal environment has changed remarkably.

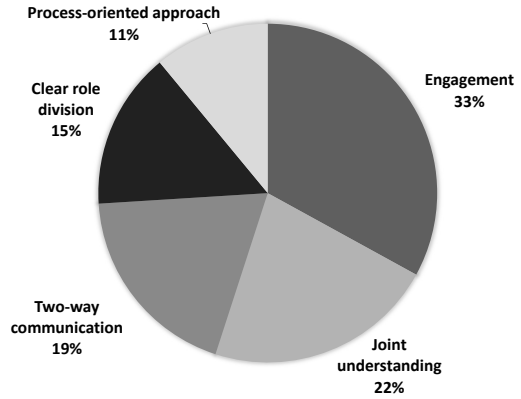

Fig. 3 Public-private cooperation success factors

In addition to the national legislation, that basically consisted of the Digital Signature Act[9], the European dimension with its directives and regulations has become relevant. Changes included new procurement and data protection rules and, finally, the implementation of the EU regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS)[10] followed by the new national legislation named Electronic Identification and Trust Services for Electronic Transactions Act in 2016[11].

During the interviews interviewees named various factors that affect PPP in the eID field. However, it is not possible to provide a complete list of factors affecting the cooperation. Therefore, we identified factors according to how often they occured in the interviews and this way determined five as most relevant, see Fig. 3. Therefore, We aim to identify existing factors and create a starting point for further critical success factors analysis.

Engagement is the most important factor since 33% of the interviewees mentioned it. Private sector representatives would like to be involved to the public sector initiatives already from the beginning. Joint understanding means that both sectors share the same basic understanding of the topic in general; that they have access to the same background information to form their opinion; but also, that they have the same understanding at the level of terminology. Two-way communication stands for an active and systematically driven

[9] https://www.riigiteataja.ee/akt/71878
[10] shorturl.at/djovX
[11] https://www.riigiteataja.ee/en/eli/527102016001/consolide

communication process where both parties provide feedback to each others' proposals. Clear role division means that all involved parties are aware of who is responsible for what. Furthermore, the interviewees brought out that it needs a process-oriented approach, which means that roles, tasks and outcomes are clearly defined already at the beginning of the project. Whenever needed, it has to be possible to engage external expertise.

We compared the identified factors with the factors found by our literature review. Four of the factors that we identified occur, under same or similar names, also in the reviewed research papers (engagement, joint understanding, two-way understanding, clear role division), however, they do not occur in that particular combination; and our research paper investigates them, to our best knowledge, for the first time in the context of eID critical infrastructure. Furthermore, the utilization of a process-oriented approach is a factor uniquely identified in this research.

4.2 Stakeholder Environment Analysis

As engagement plays an important role in public-private cooperation, we analyzed the stakeholders' environment whether all relevant parties were involved. Therefore, to identify the stakeholders and make detailed conclusions, we asked the interviewees whether all relevant stakeholders in the eID field were engaged to the process or whether there were any missing or superfluous parties. Two of the interviewees said that the practice that associations represent the interests of their members is not sufficient for them and that companies should be invited to participate directly in eID-related discussions. Currently, the Estonian Association of Information Technology and Telecommunications (Estonian Association of Information Technology and Telecommunications, 2019) represents the interests of more than ninety IT companies and the Estonian Banking Association represents the interests of all financial service providers in the local market.

Therefore, it is not reasonable to involve professional association representatives but certain companies directly. Interviewees also pointed out that engagement is not only about participation in diverse events but about active participation that needs time and extra effort.

One interviewee brought out that currently only two main public IT service providers (SMIT and the Centre of Registers and Information Systems) were engaged to the discussions. Other public sector IT service providers, for example IT Centre under the governing area of the Ministry of Finance, was not part of the process. AsIT authorities present service provider view from the public sector side, it is important to include them.

The eID card manufacturer plays a crucial role in introducing new trends to public and private sector experts. Therefore, the eID card manufacturer should participate actively in discussions related to eID systems.

Four interviewees emphasized that policy makers have to be actively involved. The interviewees also found that it is not necessary to engage so many managers and that it would be beneficial to involve more experts. Furthermore, the interviews brought out that standardization bodies are currently missing.

4.3 Improvement Proposals

4.3.1 General Proposals

In order to answer our second research question, we asked from the interviewees their proposals on how to improve the cooperation between the public and the private sector in the field of eID, see Table 7. To ensure the anonymity of the interviewees, the column numbers in Table 7 do not refer to concrete interviewees. Altogether, the interviewees made twelve proposals. Some of the proposals were made multiple times. We are convinced that all of these proposals can help to ease the communication between the two sectors.

Community Building

Five interviewees found that it is important to invest in active and continuous community building. They found that it is not enough when public and private parties get together during specific projects or one-time events. Community building inside the sector (in this case eID field) has to be continuous process.

Overall Architectural Vision

Another proposal made by five interviewees, was the need for an overall architectural vision. In regard of this, the interviewees found that there

	Interviewees (anonymised)												
Proposals	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**Total**
Community building	×						×		×	×	×		5
General architectural vision		×	×	×		×	×						5
Expert involvement in decision making		×		×				×				×	4
Joint understanding		×	×		×		×						4
Systematic meeting culture		×			×					×	×		4
External expert involvement	×	×				×							3
Two-way feedback		×		×	×								3
Inclusion of strategic agreements	×							×					2
Internal communication	×									×			2
Clear role division		×	×										2
Sector specific strategies		×											1
Academic sector engagement							×						1

Table 7 Proposals to improve collaboration between the public and the private sector, together with an indication which interviewee (1. to 12.) has made which proposal (interviewees are anonymised, i.e., numbers do not identify concrete interviewees).

is a need for a role who holds the responsibility for the overall eID architecture of the whole eID ecosystem. Such eID architecture consists of several layers and components, and every stakeholder is responsible for certain parts of the ecosystem. It is important that always at least one of the parties has a complete overview of the eID architecture so that it is always possible to understand the relations and dependencies between architectural components in support of the continuous development of the eID architecture. The state needs to have a clear understanding of the dependencies between the existing e-services and the eID ecosystem.

Expert Involvement in Decision Making

Four interviewees found that it is important to engage experts to strategic discussions. It is not sufficient if high- or mid-level managers meet and discuss strategic matters. Therefore, public and private sector eID experts have to be engaged in the discussions and involved in the decision making process.

Joint Understanding

Joint understanding was mentioned by four interviewees. They emphasized that the two sectors have to be able to "speak same the language" and understand each other. It is important to take into account the existing context not historical background. Furthermore, the interviewees found that public and private sector experts use terminology differently. The same term can have various interpretations. Therefore, the use of terminology has to be harmonized.

Systematic Meeting Culture

Four interviewees mentioned that there is a need for regular meetings between the two sectors in the eID field. In addition to regular meetings, there is a need for strategic communication at least once a year taking into account the budget planning cycle.

External Expert Involvement

Three interviewees found that independent external experts should be involved in eID-related projects. Moreover, they found that it is good to engage third parties as consultants in the preparation of vision documents and to moderate strategic discussions and workshops in a systematic manner. Furthermore, in case of a larger project (such as strategy building or revision), it is better to have a dedicated project manager who coordinates the whole process.

Two-Way Feedback

Three interviewees brought out that giving and receiving feedback is very important. Private sector representatives expect to get feedback on their comments by the public authorities. Also public sector authorities would like to get input from the private sector to implement several projects or solve critical incidents. Furthermore, it would be

helpful, if the private sector is asked early what they would prefer to contribute and what they expect from the public sector.

Inclusion of Strategic Agreements

Two experts found that strategical agreements between the two sectors should be included in the nationally relevant strategic documents, in support of strengthening these agreements. In other words, political strategies should reflect existing agreements between the two sectors.

Internal Communication

Improvement of internal communication was mentioned by two experts. Internal communication in this context means communication between the public and private parties in the field of eID. Experts found that there is a need to improve internal communication inside the sector from both perspectives.

Clear Role Division

Two interviewees found that the division of roles has to be clarified in the field of eID. This means that all involved parties understand their responsibilities and agree on what both sectors can expect from each other.

Sector Specific Strategies

One interviewee emphasized the importance of sector specific strategic documents. Overall vision documents are essential, however, also each field needs detailed direction. Moreover, at strategic level, it should be common practice that the public and the private sector develop sector specific strategies together.

Academic Sector Engagement

One interviewee brought out that, in addition to the public and private sector, academic sector representatives should be involved in eID specific discussions. The interviewee suggested that the academic sector could be a bridge between the public and the private sector.

4.3.2 Proposals for Alternative Cooperation Formats

In addition to the suggestions in Sect. 4.3.1, the interviewees proposed various alternative cooperation formats that could improve the public-private cooperation in the field of eID. Altogether, the interviewees made six alternative cooperation proposals, see Table 8. Similarly to Table 7, the column numbers in Table 8 do not refer to concrete interviewees.

Moderated Workshops

Six interviewees considered moderated workshops as an effective way to improve public-private cooperation. According to the interviewees, moderated workshops should be regular part of the interaction between the two sectors, especially in case of strategic discussions. The moderator should be a professional from outside the eID domain.

Agile Collaboration

One interviewee suggested the collaboration approach of the CA/Browser Forum[12] (Certification Authority / Browser Forum). The CA/Browser Forum is a voluntary consortium of certification authorities and software vendors selling Internet browser software, operating systems etc. Their agile collaboration approach heavily relies on forums and ballots and allows experts from the public and the private sector to engage in the decision-making process. As collective intelligence systems (Suran et al, 2020) that support such forms of agile collaboration become more and more important, we predict, that they are also well-suited candidates for collaboration in the field of eID.

Brainstorming

One interviewee found that public-private organisations need to brainstorm together at least once a year. This is especially important in the strategy building process. The interviewee suggested that those brainstorming meetings should be facilitated by external professionals.

Visualization

One interviewee pointed out that documents and other handed out materials should contain more

[12] https://cabforum.org/

	Interviewees (anonymised)												
Cooperation Format	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**Total**
Moderated workshops	×	×				×	×			×	×		6
CA/Browser Forum format			×										1
Brainstorming									×				1
Visualization						×							1
Engagement of volunteers										×			1
Software development principles					×								1

Table 8 Alternative cooperation format proposals, together with an indication which interviewee (1. to 12.) has made which proposal (interviewees are anonymised, i.e., numbers do not identify concrete interviewees).

visualizations to provide a quick overview for the experts. Moreover, the overall architecture should be visualized, together with dependencies between the architectural components.

Engagement of Volunteers

Many successful cooperation formats are centered around volunteers. There are also IT enthusiasts that are interested in the field of eID. Therefore, one interviewee suggested engaging IT volunteers to improve quality and to increase innovation in the eID domain.

Long-Term Product Plan

From a strategical viewpoint, one interviewee would like to have established a technological product discipline such as found in the long-term software life-cycle plans of, e.g., operation system providers. This would mean that the public sector would announce and follow long-term plans for the versions of its eID solutions; hand-in-hand with some long-term guarantee of respective technological support. This would be important, since any change to an eID solution in the public sector triggers a cascade of necessary changes in the systems of the private sector, since the systems in the private sector have to comply to the systems in the public sector. Therefore, private sector players are severely challenged, whenever changes to a public sector system are announced on a short-term or even ad-hoc basis.

5 Conclusion

Estonia is one of the first countries, where digital authentication and digital signing are part of the state-critical infrastructure. This makes our research relevant for other countries where eID solutions are about to become part of the state-critical infrastructure.

The aim of this paper was to identify the factors that affect public-private cooperation and to analyze several aspects of PPP in the context of the eID field. We aim to improve collaboration between the two sectors in managing state-critical infrastructure components including electronic authentication and digital signing. Previous studies focused on large-scale infrastructure sectors such as water and electricity or on analysing the experience of developing countries. Estonia is one of the first countries where digital authentication and signing are part of the state-critical infrastructure. Therefore, we focus on the case of Estonia.

Based on qualitative interviews, we identified five top factors that affect public-private cooperation in the field of electronic identity: engagement, joint understanding, two-way communication, clear division of roles and following a process-oriented approach. Here, the first four factors are well-reflected in the existing literature, albeit not in that particular combination, and the fifth factor, i.e., following a process-oriented approach, has been genuinely found by our study.

The practice of e-government in Estonia shows a series of specific aspects, compare with Bharosa et al (2020): government tends to be trusted by the citizens; there exists an exhaustive set of stable legal assets; in general, e-government is subject to central steering; and, governmental bodies and authorities are oriented towards innovation in service of the whole society. These specific aspects need to be considered, when generalizing our results. In any case, we are convinced that the found factors provide a valuable reference in the analysis and comparison with other countries' practices.

Based on our research results, further research can be conducted in studying the several proposals made by the interviewees in practice.

We analyzed that usual cooperation formats such as meetings and working groups do not sufficiently support collaboration between public and private eID stakeholders. To overcome this, it would be interesting to analyse the utilization of collective intelligence systems in service of more agile collaboration and decision making. Moreover, further research should be conducted on how to engage IT volunteers in critical infrastructure management.

Our research compiles essential success factors for public-private cooperation from various research projects and demonstrates that the critical success factors in the field of eID are not significantly different from those affecting the management of other state-critical infrastructure components. Furthermore, the Estonian case demonstrates that common understanding between the public and the private sector starts already at the level of terminology. We suggest that knowledge of the found sector-specific factors, when combined with innovative cooperation formats, can add significant additional value to the management of state-critical infrastructure.

Conflict of Interest

No conflicts of interest to declare.

References

Alcaraz C, Zeadally S (2015) Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection 8:53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Alinaitwe H, Ayesiga R (2013) Success factors for the implementation of public-private partnerships in the construction industry in Uganda. Journal of Construction in Developing Countries 18(2):1–14

Ameyaw EE, P.C. Chan A (2016) Critical success factors for public-private partnership in water supply projects. Facilities 34(3/4):124–160. https://doi.org/10.1108/f-04-2014-0034

Ansper A (2001) E-State From a Data Security Perspective. Tallinn University of Technology, Faculty of Systems Engineering, Department of Automation, Tallinn

Ansper A, Buldas A, Freudenthal M, et al (2013) High-performance qualified digital signatures for X-Road. In: Nielson HR, Gollmann D (eds) Proceedings of NordSec 2013 – the 18th Nordic Conference on Secure IT Systems, Lecture Notes in Computer Science, vol 8208. Springer, pp 123–138

Ayo-Vaughan E, Poon J, Ibem E (2019) Critical success factors for public-private partnerships (ppps) in airport infrastructure in Lagos, Nigeria. International Journal of Civil Engineering and Technology 10(2):2441–2453

Babatunde SO, Opawole A, Akinsiku OE (2012) Critical success factors in public-private partnership (PPP) on infrastructure delivery in Nigeria. Journal of Facilities Management 10(3):212–225. https://doi.org/10.1108/14725961211246018

Babatunde SO, Perera S, Zhou L, et al (2016) Stakeholder perceptions on critical success factors for public-private partnership projects in Nigeria. Built Environment Project and Asset Management 6(1):74–91. https://doi.org/10.1108/bepam-11-2014-0061

Bharosa N, Lips S, Draheim D (2020) Making e-government work: Learning from the Netherlands and Estonia. In: Hofmann S, Csáki C, Edelmann N, et al (eds) Proceedings of ePart'2020 – the 12th IFIP WG 8.5 International Conference on Electronic Participation, Lecture Notes in Computer Science, vol 12220. Springer International Publishing, pp 41–53, https://doi.org/10.1007/978-3-030-58141-1_4

Chan AP, Lam PT, Chan DW, et al (2010) Critical success factors for ppps in infrastructure developments: Chinese perspective. Journal of construction engineering and management 136(5):484–494

Cheung E, Chan APC, Kajewski S (2012a) Factors contributing to successful public private

partnership projects. Journal of Facilities Management 10(1):45–58. https://doi.org/10.1108/14725961211200397

Cheung E, Chan APC, Lam PTI, et al (2012b) A comparative study of critical success factors for public private partnerships (ppp) between Mainland China and the Hong Kong Special Administrative Region. Facilities 30(13/14):647–666. https://doi.org/10.1108/02632771211273132

Creswell J (2014) Research design. Qualitative, Quantitative and Mixed Methods Approaches. SAGE Publications, Inc., 4th ed. International Student Edition

Das Aundhe M, Narasimhan R (2016) Public private partnership (PPP) outcomes in e-government – a social capital explanation. International Journal of Public Sector Management 29(7):638–658. https://doi.org/10.1108/IJPSM-09-2015-0160

Debela G (2019) Critical success factors (CSFs) of public–private partnership (PPP) road projects in Ethiopia. International Journal of Construction Management pp 1–12. https://doi.org/10.1080/15623599.2019.1634667

Dithebe K, Aigbavboa C, Thwala W, et al (2019) Factor analysis of critical success factors for water infrastructure projects delivered under public–private partnerships. Journal of Financial Management of Property and Construction 24(3):338–357. https://doi.org/10.1108/JFMPC-06-2019-0049

Draheim D (2021) Data exchange for digital government: Where are we heading? In: Bellatreche L, Dumas M, Karras P, et al (eds) Proceedings of ADBIS '2021 – the 25th European Conference on Advances in Databases and Information Systems. Springer, no. 12843 in LNCS, pp 7–12

Draheim D, Nathschläger C (2008) A context-oriented synchronization approach. In: Electronic Proceedings of the 2nd Intl. Workshop in Personalized Access, Profile Management, and Context Awareness: Databases (PersDB 2008) in Conjunction with the 34th VLDB Conference, pp 20–27

Draheim D, Krimmer R, Tammet T (2021) Architecture of digital government ecosystems: from ICT-driven to data-centric. Transactions on Large-Scale Data- and Knowledge-Centered System, Special Issue In Memory of Univ Prof Dr Roland Wagner XLVIII:165–195

Dunn-Cavelty M, Suter M (2009) Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. International Journal of Critical Infrastructure Protection 2(4):179–187. https://doi.org/10.1016/j.ijcip.2009.08.006

E-Governance Academy (2016) E-Governance in Practice. E-Governance Academy, https://ega.ee/wpcontent/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf

European Commission (2016) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Commission

Filiol E, Gallais C (2014) Critical infrastructure: Where we stand today. In: Proceedings of the 9th International Conference on Cyber Warfare and Security, West Lafayette, pp 47–57

Firmino SI (2018) Critical success factors of public-private partnerships: political and institutional aspects. case study of highways in portugal. Revista de Administração Pública 52:1270–1281. https://doi.org/10.1590/0034-761220170228

Ghribi S, Hudon PA, Mazouz B (2019) Risk factors in IT public–private partnership projects. Public Works Management and Policy 24(4):321–343. https://doi.org/10.1177/1087724X18823009

Hai DT, Toan NQ, Van Tam N (2022) Critical success factors for implementing PPP infrastructure projects in developing countries: the case of vietnam. Innovative Infrastructure Solutions 7(1):1–13. https://doi.org/10.1007/s41062-021-00688-6

Hsueh CM, Chang LM (2017) Critical success factors for ppp infrastructure: perspective from taiwan. Journal of the Chinese Institute of Engineers 40(5):370–377. https://doi.org/10.1080/02533839.2017.1335619

Ismail S (2013) Critical success factors of public private partnership (PPP) implementation in Malaysia. Asia-Pacific Journal of Business Administration 5(1):6–19. https://doi.org/10.1108/17574321311304503

Jacobson C, Ok SO (2008) Success factors: Public works and public-private partnerships. International Journal of Public Sector Management 21(6):637–657. https://doi.org/10.1108/09513550810896514

Kalja A (2008) The X-Road: a key interoperability component within the state information system. In: Information technology in public administration of Estonia – yearbook 2007. Ministry of Economic Affairs and Communications Estonia, pp 19–20

Kalja A (2012) The first ten years of X-Road. In: Kastehein K (ed) Information technology in public administration of Estonia – yearbook 2011/2012. Ministry of Economic Affairs and Communications Estonia, pp 78–80

Kalja A, Robal T, Vallner U (2015) New generations of Estonian eGovernment components. In: Proceedings of PICMET'2015 – the 15th Portland International Conference on Management of Engineering and Technology. IEEE, pp 625–631

Kalvet T, Toots M, Krimmer R (2018) Contributing to a digital single market for Europe: barriers and drivers of an EU-wide once-only principle. In: Proceedings of DG.O'2018 – the 19th Annual International Conference on Digital Government Research. ACM, pp 45:1–45:8

Koppenjan J, Groenewegen J (2005) Institutional design for complex technological systems. International Journal of Technology, Policy and Management 5(3):240–257. https://doi.org/10.1504/IJTPM.2005.008406

Li B, Akintoye A, Edwards P, et al (2005) Critical success factors for PPP/PFI projects in the UK construction industry. Construction Management and Economics 23(5):459–471. https://doi.org/10.1080/01446190500041537

Lips S, Tsap V, Pappel I, et al (2018) Key factors in coping with large-scale security vulnerabilities in the eID field. In: Kõ A, Francesconi E (eds) Proceedings of EGOVIS'2018 - the 7th International Conference on Electronic Government and the Information Systems Perspective, Lecture Notes in Computer Science, vol 11032. Springer, Cham, pp 60–70, https://doi.org/10.1007/978-3-319-98349-3_5

Lips S, Aas K, Pappel I, et al (2019) Designing an effective long-term identity management strategy for a mature e-state. In: Kõ A, Francesconi E, Anderst-Kotsis G, et al (eds) Proceedings of EGOVIS'2019 – the 8th Conference on Electronic Government and the Information Systems Perspective, Lecture Notes in Computer Science, vol 11709. Springer, Berlin, Heidelberg, New York, pp 221–234, https://doi.org/10.1007/978-3-030-27523-5_16

Medaglia R, Hedman J, Eaton B (2017) It takes two to tango: Power dependence in the governance of public-private e-government infrastructures. In: Proceedings of ICIS'2017 – 38th International Conference on Information Systems: Transforming Society with Digital Innovation. AIS

Muhammad Z, Johar F (2018) Critical success factors of public–private partnership projects: a comparative analysis of the housing sector between Malaysia and Nigeria. International Journal of Construction Management 19(3):257–269. https://doi.org/10.1080/15623599.2017.1423163

Muldme A, Pappel I, Lauk M, et al (2018) A survey on customer satisfaction in national electronic ID user support. In: Proceedings of ICEDEG'2018 – the 5th International Conference on eDemocracy & eGovernment. IEEE, pp 31–37, https://doi.org/10.1109/ICEDEG.2018.8372374

Mulyani S (2021) Critical success factors in public-private partnership. Journal of Accounting Auditing and Business-Vol 4(1):81–86. https://doi.org/10.24198/jaab.v4i1.31953

Osei-Kyei R, Chan APC (2015) Review of studies on the critical success factors for public–private partnership (PPP) projects from 1990 to 2013. International Journal of Project Management 33(6):1335–1346. https://doi.org/10.1016/j.ijproman.2015.02.008

Osei-Kyei R, Chan APC (2019) Model for predicting the success of public–private partnership infrastructure projects in developing countries: a case of Ghana. Architectural Engineering and Design Management 15(3):213–232. https://doi.org/10.1080/17452007.2018.1545632

Owolabi H, Oyedele L, Alaka H, et al (2020) Critical success factors for ensuring bankable completion risk in PFI/PPP megaprojects. Journal of Management in Engineering 36(1):1–16. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000717

Paide K, Pappel I, Vainsalu H, et al (2018a) On the systematic exploitation of the Estonian data exchange layer X-Road for strengthening public private partnerships. In: Kankanhalli A, Ojo A, Soares D (eds) Proceedings of ICEGOV'18 – the 11th International Conference on Theory and Practice of Electronic Governance. Association for Computing Machinery, pp 34–41, https://doi.org/10.1145/3209415.3209441

Paide K, Pappel I, Vainsalu H, et al (2018b) On the systematic exploitation of the Estonian data exchange layer X-Road for strengthening public private partnerships. In: Proceedings of ICEGOV'2018 – the 11th International Conference on Theory and Practice of Electronic Governance. ACM, pp 34–41

Petersson AM, Lundberg J (2016) Applying action design research (ADR) to develop concept generation and selection methods. Procedia CIRP 50:222–227. https://doi.org/10.1016/j.procir.2016.05.024

Pursiainen C (2018) Critical infrastructure resilience: A Nordic model in the making? International Journal of Disaster Risk Reduction 27:632–641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Regulation no. 105 (2016) The Data Exchange layer of Information Systems. Government of the Republic of Estonia, https://www.riigiteataja.ee/akt/106082019017

Regulation no. 196 (2004) Statute of the Ministry of Foreign Affairs. Government of the Republic of Estonia, https://www.riigiteataja.ee/akt/123122021020

Regulation no. 28 (2011) Statute of the Estonian Information System Authority. Minister of Economic Affairs and Communications, https://www.riigiteataja.ee/akt/122022022003

Regulation no. 323 (2002) Statute of the Ministry of the Economic Affairs and Communications. Government of the Republic of Estonia, https://www.riigiteataja.ee/akt/123102021005

Regulation no. 33 (2014) Statute of the Estonian Police and Border Guard Board. Minister of the Interior, https://www.riigiteataja.ee/akt/115062022010

Regulation no. 39 (2012) Statute of the Ministry of the Interior. Government of the Republic of Estonia, https://www.riigiteataja.ee/akt/123032022009

Regulation no. 8 (2020) Statute of the IT and Development Centre of the Ministry of the Interior of Estonia. Minister of the Interior, https://www.riigiteataja.ee/akt/130102020029

Sanni AO (2016) Factors determining the success of public private partnership projects in Nigeria. Construction Economics and Building 16(2):42–55. https://doi.org/10.5130/AJCEB.v16i2.4828

Saputro R, Pappel I, Vainsalu H, et al (2020) Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study. In: Proceedings of ICEDEG 2020 – the 7th International Conference on eDemocracy & eGovernment. IEEE, pp 216–222,

Schuppert GF (2015) Governance. In: Wright JD (ed) International Encyclopedia of the Social & Behavioral Sciences (Second Edition), second edition edn. Elsevier, Oxford, p 292–300, https://doi.org/https://doi.org/10.1016/B978-0-08-097086-8.75020-3

Sehgal R, Dubey AM (2019) Identification of critical success factors for public–private partnership projects. Journal of Public Affairs 19(4):e1956

Sein MK, Henfridsson O, Purao S, et al (2011) Action design research. MIS Quarterly 35(1):37–56. https://doi.org/10.2307/23043488

Surachman EN, Handayani D, Suhendra M, et al (2020) Critical success factors on PPP water project in a developing country: Evidence from Indonesia. The Journal of Asian Finance, Economics, and Business 7(10):1071–1080. https://doi.org/10.13106/JAFEB.2020.VOL7.NO10.1071

Suran S, Pattanaik V, Draheim D (2020) Frameworks for collective intelligence: A systematic literature review. ACM Computing Surveys 52(1):1–36

Tang L, Shen Q, Cheng EWL (2010) A review of studies on public–private partnership projects in the construction industry. International Journal of Project Management 28(7):683–694. https://doi.org/10.1016/j.ijproman.2009.11.009

Tawalare A, Laishram B, Thottathil F (2020) Relational partnership in public construction organizations: Front-line employee perspective. Journal of Construction Engineering and Management 146(1):1–17. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001723

Tepandi J, Lauk M, Linros J, et al (2017) The data quality framework for the Estonian public sector and its evaluation. Transactions on Large-Scale Data- and Knowledge-Centered Systems 35:1–26

Tsap V, Lips S, Draheim D (2020a) Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In: Kö A, Francesconi E, Kotsis G, et al (eds) Proceedings of EGOVIS'2020 – the 9th International Conference on Electronic Government and the Information Systems Perspective, Lecture Notes in Computer Science, vol 12394. Springer, Cham, pp 159–173, https://doi.org/10.1007/978-3-030-58957-8_12

Tsap V, Lips S, Draheim D (2020b) eID public acceptance in Estonia: towards understanding the citizen. In: Eom SJ, Lee J (eds) Proceedings of dg.o'20 – the 21st Annual International Conference on Digital Government Research: Intelligent Government in the Intelligent Information Society. Association for Computing Machinery, pp 340–341, https://doi.org/10.1145/3396956.3397009

UN Department of Economic and Social Affairs (2018) United Nations E-Government Survey 2018 – Gearing e-Government to Support Transformation Towards Sustainable and Resilient Societies. United Nations, New York

UN Department of Economic and Social Affairs (2020) E-Government Survey 2020 – Digital Government in the Decade of Action for Sustainable Development. United Nations, New York

Vaismoradi M, H. T, Bondas T (2013) Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. Nursing and Health Sciences 15:398–405. https://doi.org/10.1111/nhs.12048

Valtna-Dvořák A, Lips S, Tsap V, et al (2021) Vulnerability of state-provided electronic identification: The case of ROCA in Estonia. In: Kö A, Francesconi E, Kotsis G, et al (eds) Proceedings of EGOVIS'2021 – the 10th International Conference Electronic Government and the Information Systems Perspective, Lecture Notes in Computer Science, vol 12926. Springer, Cham, pp 73–85

Węgrzyn J, et al (2016) The perception of critical success factors for PPP projects in different stakeholders groups. Entrepreneurial Business and Economics Review 4(2):81–92. https://doi.org/10.15678/EBER.2016.040207

Willemson J, Ansper A (2008) A secure and scalable infrastructure for inter-organizational data exchange and eGovernment applications. In: Proceedings of the Third International Conference on Availability, Reliability and Security 2008, pp 572–577

Williamson OE (1979) Transaction cost economics: the governance of contractual relations. The Journal of Law & Economics 22(2):233–261

Williamson OE (1998) Transaction cost economics: How it works; where it is headed. De Economist 146(1):25–58

Wróbel R (2019) Dependencies of elements recognized as critical infrastructure of the state. Transportation Research Procedia 40:1625–1632. https://doi.org/10.1016/j.trpro.2019.07.225

Yin RK (2011) Applications of case study research. Sage

Zhang X (2005) Critical success factors for public–private partnerships in infrastructure development. Journal of Construction Engineering and Management 131(1):3–14. https://doi.org/10.1061/(asce)0733-9364(2005)131:1(3)

Silvia Lips

Silvia Lips is an early stage researcher and PhD candidate in the Information Systems Group at Tallinn University of Technology (Taltech). She also works as an eID expert at the Estonian Information System Authority and is member of the eIDAS Cooperation Network at the European Commission. Silvia holds LL.M (cum laude) in law and MSc (cum laude) in e-governance services and technologies. More than 15 years, she has been active in the eID field and led various eID related projects, including the Estonian eID card procurement project, mobile-ID procurement project, Estonian e-passport procurement project, and Estonian electronic identity strategy building. Her current research focuses on the mutual recognition and evaluation of eID schemes.

Valentyna Tsap

Valentyna Tsap is an Analyst and Lead Consultant for digital identity projects at Cybernetica, Digital Identity Technologies Department. She has acquired a doctoral degree in Computer Science. She defended her doctoral thesis on the topic "eID public Acceptance: Success Factors, Citizen Perception, and Impact of Electronic Identity" in spring of 2022. Previously, she worked as a researcher at Tallinn University of Technology where she was involved in a number of international projects on the development of e-government systems and university curricula.

Nitesh Bharosa

Nitesh Bharosa is Full professor of GovTech and Public Service Innovation at the Faculty of Technology, Policy and Management of Delft University of Technology. His research focusses on designing and governing GovTech – digital innovations for the public sector. Nitesh is also the academic director of Digicampus – a quadruple helix ecosystem for public service innovation. At Digicampus, public agencies, GovTech companies, research institutes, and citizen groups co-create and experiment with the next generation of public services, using state-of-the-art information technologies such as digital identities, data wallets, cyber-trust services and AI (www.digicampus.tech).

Robert Krimmer

Robert Krimmer is an expert in digital transformation and is focused on digital transformation, cross-border e-services, electronic participation and democracy, as well as e-voting, and all issues further developing a digital society. In 2019, he has been mentioned as one of the top 16 academics within the list of 100 most influential people in digital government by Apolitical. Between 2017 and 2021 Robert coordinated TOOP, the EU H2020 large-scale pilot on exploring and demonstrating the feasibility of the once-only principle involving 50+ partners from more than 20 countries inside and outside the European Union. Further, he was member of the group of experts to the Council of Europe Ad-Hoc Committee on Electronic Voting (CAHVE) which edited the recommendation on legal, technical and operational standards for Electronic Voting Rec(2017)5. Also, he was one of the lead experts for the Council of Europe Ad-Hoc Committee on Electronic Democracy and drafted

Annex 1 of the CoE Recommendation (2009) on e-Democracy. Before returning to academia, Robert was OSCE/ODIHR's first senior adviser on new voting technologies. In the past he advised a number of international organizations, including CoE, OSCE/ODIHR, UNESCO, UNDP, WHO, ITU, IFAD, AfDB, the European Commission or AWEB on matters regarding digital transformation.

Tanel Tammet

Tanel Tammet is a full professor of applied artificial intelligence at Tallinn University of Technology. His main research interests include crowdsourced knowledge bases, automated reasoning and commonsense reasoning. He has also worked in the area of cybersecurity and has been involved in numerous large commercial and public sector IT projects. Tanel was one of the initiators of the Estonian X-ROAD interoperability framework and has helped to develop several other core IT infrastructure systems in Estonia.

Dirk Draheim

Dirk Draheim received the PhD from Freie Universität Berlin and the habilitation from Universität Mannheim, Germany. Currently, he is full professor of information society technology at Tallinn University of Technology and head of the Information Systems Group, Tallinn University of Technology, Estonia. The Information Systems Group conducts research in large and ultra-large-scale IT systems. He is also an initiator and leader of numerous digital transformation initiatives. Dirk is author of the Springer books "Business Process Technology", "Semantics of the Probabilistic Typed Lambda Calculus" and "Generalized Jeffrey Conditionalization", and co-author of the Springer book "Form-Oriented Analysis".

Appendix 2

II

S. Lips, N. Vinogradova, R. Krimmer, and D. Draheim. Re-shaping the EU digital identity framework. In *the 23rd Annual International Conference on Digital Government Research*, dg.o 2022, page 13–21, New York, NY, USA, 2022. Association for Computing Machinery

Re-Shaping the EU Digital Identity Framework

Silvia Lips
silvia.lips@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

Natalia Vinogradova
natalia.vinogradova@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

Robert Krimmer
robert.krimmer@ut.ee
Johan Skytte Institute of Political Studies, University of Tartu
Tartu, Estonia

Dirk Draheim
dirk.draheim@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

ABSTRACT

Electronic authentication and digital signature are the base components of the European Union (EU) Digital Single Market. The area is regulated by the eIDAS (electronic identification and trust services for electronic transactions in the internal market) regulation that is compulsory for all Member States since 2018. Despite the Member States' efforts, the regulation implementation has not been as successful as expected. Therefore, the European Commission initiated the eIDAS revision process in the second half of 2020. Based on the collected feedback, the Commission proposed in July 2021 the first draft of the renewed eIDAS regulation establishing the European Digital Identity framework. The aim of this research is to analyze the feedback provided by different countries and sectors in the eIDAS review process (156 pages of material) and evaluate their correspondence to the Commission proposal. The research follows the exploratory case study methodology and we use thematic analysis for the evaluation. The outcome of this study shows whether all relevant expectations of the interested parties are covered by the Digital Identity Framework proposal and the research results are a valuable input for the Commission as the debate over the eIDAS regulation draft is ongoing.

CCS CONCEPTS

• **Social and professional topics** → **Government technology policy**.

KEYWORDS

eIDAS, electronic authentication, electronic identity, implementation challenges, identity management, digital signature

, ,

ACM ISBN 978-1-4503-9749-0/22/06.
https://doi.org/10.1145/3543434.3543652

ACM Reference Format:
Silvia Lips, Natalia Vinogradova, Robert Krimmer, and Dirk Draheim. 2022. Re-Shaping the EU Digital Identity Framework. In . ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3543434.3543652

1 INTRODUCTION

The European Digital Single Market is one of the backbones of the EU and part of the EU single market strategy [1]. The Digital Single Market largely depends on the electronic identities of Member States and provides trust services regulated by the eIDAS, electronic identification and trust services for electronic transactions in the internal market, regulation. EU citizens need to be able to use their national eIDs for the services in other EU Member States. Meanwhile, there should be a guarantee that different electronic authentication schemes operate across borders without limitations inside the EU and given digital signatures are legally binding in all Member States [21]. According to the European Commission eIDAS impact assessment report, the ongoing COVID pandemic situation has sped up the need for digitization by seven years [2]. This means that the need for digitization and the importance of a well functioning EU Digital Single Market has become even more relevant.

To enable an interoperable and secure e-service provision, cross-border authentication, and acceptance of electronic signatures, the EC adopted, on the 23rd of July 2014, the regulation on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS) [3]. Until 2016, the adoption of this regulation was voluntary for the Member States. Since September 2018 it has become mandatory [12].

Unfortunately, despite the Member States' efforts, the implementation of the eIDAS regulation has not been simple, and the EU digital market is not operating as expected [12]. Every Member State has its individual digital market operating within the national legal framework. This variety of different digital identification solutions in the EU has gradually become an obstacle in terms of cross-border interoperability in the European internal market [17, 22]. In four years since mandatory implementation, only 59% of the EU population has a chance to benefit from the EU Digital

[1] Single Market and Standard. https://ec.europa.eu/growth/single-market_en
[2] European Commission. eIDAS Impact Assessment Report. https://ec.europa.eu/newsroom/dae/redirection/document/76618
[3] eIDAS regulation. Available: http://data.europa.eu/eli/reg/2014/910/oj

Single Market [4]. Therefore, the EC initiated, in the second half of 2020, the eIDAS public consultation process to collect the interested parties' feedback about the existing regulation and related challenges. The aim was to revise the regulation. After analysing the feedback, the EC proposed, in July 2021, an amended version of the eIDAS regulation, which included the European digital identity framework.

This research focuses on the analysis of the EC's proposal and its correspondence to the feedback received during the public consultation procedure. The aim is to find out, weather the proposal covers public and private sector authorities' main concerns towards the eIDAS regulation, and to provide input to the ongoing eIDAS revision process.

Based on the aim of this research, the main research questions are:

- What are the public and private sector authorities' main amendment expectations towards the eIDAS regulation?
- How do the eIDAS regulation amendments proposed by the European Commission meet the public and private sector authorities' expectations?

Sect. 2 provides an overview of electronic identity and eIDAS related literature. Sect. 3 gives an overview of the eIDAS regulation and its state of play, including the EC eIDAS revision proposal. Sect. 4 describes the research methodology and data collection procedure and analysis method. Sect. 5 presents the research findings from the private and public sector perspective. In Sect. 6, we analyze the the correlation of interested parties' feedback to the eIDAS regulation proposal. Sect. 7 provides an insight to the research limitations and to the future research perspective and we conclude the paper in Sect. 8.

2 LITERATURE REVIEW

The electronic identity is a central concept for the development and operation of digital government [8, 23] and e-commerce [15]. For instance, the eID became a part of the Estonian critical infrastructure [22], and the state itself is the eID primary end-user and highly dependent on its eID [25]. This section provides an overview of the eID and eIDAS related literature that is relevant from this research perspective with the focus on the obstacles and triggers of the EU digital identity implementation from the public and private sector authorities' perspective.

Despite the importance of the concept, there is no universal definition for electronic identity. The literature indicates broad and narrow concepts of identity in the digital space. For instance, Hoikkanen defines the term eIdentity as a "data set related to a personal or collective identity stored and transferred in the electronic systems" [7]. It is worth mentioning that Hoikkanen uses the terms electronic identity, digital identity and eID interchangeably [7]. At the same time, Khatchatourov uses the term eID only in the context of the eIDAS Regulation [8]. Contrary, van Dijck and Jacobs specify eIDs as "digital solutions to prove one's identity", where the main functionalities of the solutions comprise authentication, login and digital signing [26]. Overall, identity in the digital space can relate to all online transactions [8]. Current work focuses on the national electronic identification (eID) and authentication schemes and trust services as part of the EU Digital Single Market.

The topic of eIDAS implementation processes in EU countries is relatively new and only partially researched. Researchers focus mainly on some specific areas or technical issues of the eIDAS [12]. For instance, among technical solutions that are examined in the framework of eID systems and eIDAS: the authentication of additional data and different cryptography solutions [14], pseudonyms and pseudonymous signature [8, 11], and integration of block-chain technology with Qualified Electronic Signatures [24]. Further, there are proposals to widen the scope of the technological solution. For example, including an electronic signature of the ICO smart contracts [27].

Furthermore, the literature analyses the national eID systems, their integration with eIDAS-Node, their further extensions, proposes alternative technical solutions. For instance, the German eID schema is broadly examined [11, 13, 14]. Further, an overview of the Italian architecture for the eIDAS-Node and connection of the eID scheme is provided [21], and the Dutch IRMA eID system is outlined [26]. Some research papers offer various applications of the eIDAS-Node in an educational context [3, 5, 6, 9]. For example, proposing an extension of the basic set of attributes by adding academic attributes as part of citizens' profiles and offer technical solutions. They claim that it would be beneficial for citizens in the education context. In particular, this would save the students' time on the application procedure and allow them to use academic services through national eID [3].

Since the provision of online services is closely related to the concerns of "security, privacy, and trust" [2] moreover, a multitude of various digital identities brings inconveniences for users and endangers their security and privacy in cyberspace [15], privacy aspects are widely discussed in the context of electronic identity, identity management and eIDAS [8, 11, 14]. For example, Kim Nguyen considers aspects of trust that are embedded in the eIDAS regulation. Firstly, he argues that the certification procedure guarantees users that the provider's services are trustworthy. The requirements for the trust services provision, the systems itself and its' elements are established in the European standards. Moreover, the certification is provided by independent third parties and supervised by national agencies. As a result of certification, all qualified trust service providers are registered in the trust lists together with the description of their services. Other criteria that would ensure trust by Nguyen are the "evaluation of the cryptography process, the definition of minimal requirements, and decentralized trust models based on transparency principles" [16].

Some researchers investigated if eIDAS is beneficial for the Member States and their national cross-border programs and e-government objectives or somewhat burdensome. Although eIDAS poses additional obligations on the Member States, they suggest that it rather supports national initiatives and projects, such as e-residency in Estonia, than challenges them. Therefore, it is beneficial for the governments to implement eIDAS [1].

Nevertheless, initial research on eIDAS implementation indicates that some countries are more successful in their endeavours, while others are hesitant and struggle with the eIDAS implementation [17]. Early comparison of national eID systems in Europe demonstrates that there are different technical and organisational

[4]European Commission. eIDAS Impact Assessment Report. https://ec.europa.eu/newsroom/dae/redirection/document/76618

elements between the systems [10], also architectural solutions of the identity systems are diverse [8]. The reason for this diversity can be clarified by the fact that each EU Member State developed their eID management system independently [21], based on the earlier systems and during "incremental innovation" and "path continuation" [10]. Each country tried to meet its' internal goals to provide secure authentication, while "interoperability with other state's eID schemes was no priority" [19].

However, identification and authentication systems of different EU countries have many similarities [20]. The diversity of the rules and systems in the electronic identity management between countries caused issues with interoperability and turned out to be an obstacle for cross-border electronic services and operation of the EU Digital Single Market [19, 21].

Generally, information systems operate on identities that connect citizens with the digital information stored in the databases. If identifiers in different databases vary, cross-referencing the information from one database to another is hindered. Therefore, the main challenge for identity management is to adapt the systems, making them interoperable and enabling cross-referencing and matching the information [4]. In other words, Member States need to implement national gateways, called eIDAS-Node, to connect to the eID systems of the other Member States [21].

Besides interoperability issues, some authors suggest that the difficulties with eIDAS implementation might be caused by the complexity of the eID concept, which encompasses more than outlined by the EU frameworks. Meanwhile, the legislation concentrates mainly on technical and legal interoperability. Other issues of a political and social nature may cause conflicts and obstacles for the eIDAS implementation. For instance, in the case of the Swedish national eID schema, it was challenging to design a new eID system having, at the same time, already existing BankID and considering opinions of all the stakeholders involved [26].

Overall, the main challenges for the member states indicated in the literature are “compliance issues”, “interpretation problems”, “different practices in Member States”, “cooperation and collaboration barriers”, and “representation of legal person” challenges [12]. Besides, the lack of knowledge among users influences the citizens' adoption rate of national eID solutions, which negatively affects the consumption of cross border electronic services. Therefore, countries should increase awareness among citizens about national eID solutions and their benefits and provide them with necessary software and qualified certificates [20].

3 eIDAS AND STATE OF PLAY

The eIDAS regulation grounded the legal foundation for electronic transactions in the EU internal market. The aim was to build trust among consumers, businesses and public authorities in the digital environment, thus boosting electronic commerce and increasing the effectiveness of public and private digital services in the European Union [5]. The regulation was adopted in July 2014 and replaced the directive 1999/93/EC on a Community framework for electronic signatures [6]. eIDAS regulation made possible to recognise other national electronic identification schemes developed in the Member States and uniform requirements for trust services were established [18].

eIDAS regulation entered into force step by step. Figure 1 illustrates in detail the eIDAS implementation timeline from the adoption to the latest European Digital Identity framework proposal. Starting from September 2015, the Member States could start voluntarily recognise each-others eIDs. In early 2016, the eID interoperability infrastructure was available for the Member States. From July 2016, provisions referring to trust service rules became effective. Finally, from the 29th of September 2018, eIDAS regulation was obligatory for all Member States and mutual recognition of eIDs became mandatory.

The eIDAS implementation comprises several stages that each country should follow. Firstly, a Member State should start eID pre-notification: officially inform the European Commission about its "intention to notify its eID scheme". Then a peer-review stage follows, where representatives of other Member States examine and assess the eID scheme. After the peer review stage, the country notifies the European Commission about its eID scheme. As soon as the information about notification is published in the Official Journal of the European Union (OJEU), but not later than 12 months, other Member States should recognise the notified eID scheme. Since the recognition, EU citizen can use the recognised eID across borders. Germany was the first country, who notified its eID scheme in 2017, followed next year by Estonia, Spain, Croatia, Belgium, Luxembourg and Italy. Currently, 17 Member States out of 27 passed the eID notification process and three countries (Czech Republic, Norway, Austria) peer-review process is ongoing. [7].

According to the eIDAS regulation, it was planned to revise the regulation and its implementation process by 01.07.2020 [8]. The EC conducted an inception impact assessment of the eIDAS revision and published a proposal to revise the eIDAS regulation on the 23rd of July 2020. According to the Inception Impact Assessment document, the EC proposed three options: [9]

- revise and slightly update the current regulation;
- extend the effect of eIDAS to the private sector;
- launch a European Digital Identity (EUid) or combine these three solutions.

During the public consultation, the EC wanted to collect feedback about the eIDAS implementation challenges from different interested parties and wanted to clarify the direction, where to develop the eIDAS regulation. The feedback was collected 23.07.2020-03.09.2020. Based on the feedback and analysis, the EC proposed in July 2021 a revised version of eIDAS - a framework for European Digital Identity [10]

[5] eIDAS regulation Available: http://data.europa.eu/eli/reg/2014/910/oj
[6] Directive 1999/93/EC. Available: http://data.europa.eu/eli/dir/1999/93/oj

[7] eID User Community.
Available: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[8] eIDAS regulation. Available: http://data.europa.eu/eli/reg/2014/910/oj
[9] Inception Impact Assesment. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=cellar:35274ac3-cd1b-11ea-adf7-01aa75ed71a1
[10] Establishing a Framework for European Digital Identity. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

Figure 1: eIDAS timeline

3.1 European Digital Identity Framework Proposal

With the revised version of eIDAS, the EC has broadened the scope of the regulation. Previously, the regulation applied to the electronic signatures, seals, time stamps, documents and registered delivery services. In addition to that, according to the regulation draft, the eIDAS applies to the electronic archiving, attestation of attributes, remote electronic signatures and seal creation devices and electronic ledgers [11].

As a major change, eIDAS proposes the legal framework for EU member states to provide EU digital identity wallets that enable users to decide, depending on the use case and needed security level, when and with whom they share various attributes (e.g. educational data, healthcare information, electronic driving license information etc.). The EU digital identity wallet should also enable electronic authentication in the online environments and giving qualified electronic signatures. The Member States must ensure the wallet solution but its usage by citizens is voluntary. The EC together with Member States will establish the technical architecture, standards and guidelines for EU digital identity wallets (also named as common toolbox) to ensure uniform approach to the wallet solution. [12] Currently, detailed discussion over the EU digital identity wallet concept between the member states is ongoing but the schedule is intense. For example, according to the regulation draft, the Member States should implement it already in June 2024.

The eIDAS proposal specifies requirements for the remote signatures to ensure secure remote signing process. The Member States should follow the European Committee for Standardization (CEN) standards that regulate the operation and authentication to remote Qualified Signature Creation Devices. Moreover, the eIDAS draft proposal aims to harmonize with the other EU legislative initiatives like the EU directive concerning measures for a high common level of security of network and information systems across the European Union (also known as EU NIS directive) [13], Cybersecurity Act [14]and Single Digital Gateway regulation [15].

To summarize the key elements of the eIDAS draft proposal:

- the name eIDAS was replaced by European Digital Identity Framework with a focus on cross-border use;
- European Digital Identity Wallet concept obligatory for Member States was introduced (including Trust Mark);
- proposal enables end users sharing of different electronic attributes within the EU;
- three new qualified trust services were added to the existing list of trust services (electronic archiving, electronic ledgers and the management of remote electronic signature and seal creation devices);
- harmonisation with other EU regulations and standards.

4 RESEARCH APPROACH

The research follows exploratory case study methodology [28]. To answer the research questions, we analysed the European Digital Identity Framework Proposal and feedback provided in the public consultation process initiated by the EC and compared them. The main changes in the eIDAS regulation proposal are presented in Sect. 3.

The feedback on the Inception Impact Assessment and eIDAS regulation was collected by EC from July 2020 to October 2020 and was made available for the public on the EC website. In total, 53 responses in different formats were received from various stakeholders. Some responses contained additional downloadable documents. This research uses only the data that was publicly available.

We extracted the collected feedback from the EC website with the help of the web scraping tool Scraper and downloaded enclosed files from the web pages. In total amount 156 pages of text. Some of the feedback needed to be translated from German, Spanish, and French into the English language for further analysis. During the feedback analysis, we focused separately on two main groups of stakeholders: the public sector representatives and private sector actors of the EU Member States.

After the data extraction, we conducted a thematic analysis of the collected data sets. We conducted the analysis in four rounds using NVIVO data analysis software. Firstly, we sorted the received feedback based on the theme from which country it was sent. Figure 2 presents the detailed data analysis model.

Secondly, we split the data into three groups (case classifications: Stakeholders): the feedback from private, public organisations and others. Initially, we expected to have the most responses from private and public organisations of EU Member States. However, the third sector organisations, EU citizens, and Non-EU organisations actively participated in the public consultation process. Therefore, we formed three groups of cases: stakeholders: public sector, private sector and others.

In the third-round we tried to find a generalisation and central themes in each stakeholder group. We applied inductive data-driven approach to find patterns and probable explanations of the challenges and triggers of eIDAS implementation and stakeholders possible expectations. During the final round, we analysed every

[11]Establishing a Framework for European Digital Identity. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
[12]Establishing a Framework for European Digital Identity. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
[13]EU NIS directive. Available: http://data.europa.eu/eli/dir/2016/1148/oj
[14]Cybersecurity Act. Available: http://data.europa.eu/eli/reg/2019/881/oj
[15]Single Digital Gateway regulation. Available: http://data.europa.eu/eli/reg/2018/1724/oj

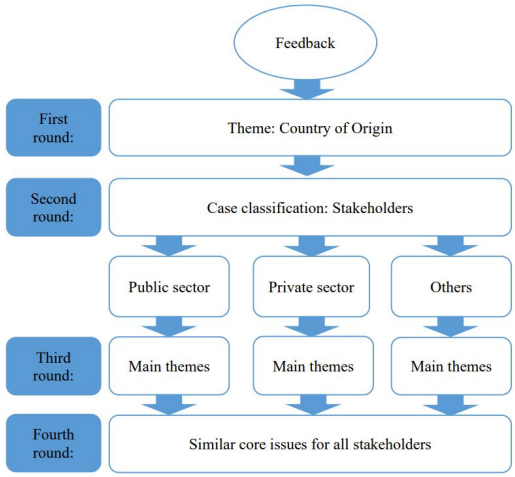

Figure 2: Data analysis model

pillar separately to identify similar problems and core issues for all stakeholders and their possible expectations towards the eIDAS regulation.

5 FINDINGS

During the first round of thematic analysis we identified from which country the feedback was received. Altogether, EC received 53 responses from 16 countries during the public consultation process. Results showed that among the respondents there were representatives of the non-EU countries (Switzerland, UK, USA, Norway), which constituted 19% of all respondents. 7% of the respondents preferred to preserve their anonymity. Therefore, the data about their countries of origin were not available. The largest number of respondents were from France (12), then followed by Germany (7), Belgium (5) and the USA (5). Table 1 represents detailed overview of the respondents by their country of origin.

During the planning phase of the research, we assumed that the largest number of all feedback would be from two types of stakeholders: public and private sector organizations of EU Member States. In contrast, the second round of the data analysis revealed that the third sector organizations, EU citizens and Non-EU organizations actively participated in the consultation process. Therefore, we split the data into three groups by stakeholders: public sector, private sector and others. The following subsections present the research results by each group.

5.1 Private Sector Feedback and Expectations

31 private sector representatives provided their feedback during the public consultation process. 22 of them were EU Member States, 8 responses from non-EU countries and one respondent preferred to stay anonymous.

Business organisations from seven EU countries out of 27 participated directly in the public consultation and sent their feedback. The largest number of responses came from France (7). German and Belgium organisations sent both five responses each. Concurrently, it is worth of mentioning that business association represented the interests of certain domain companies from a range of countries. Large companies (250 employees and more) constituted 33% of all respondents from EU countries. Small (10 to 49 employees) and micro (1 to 9 employees) organisations contributed equally with a 24% participation rate of all EU companies. Medium companies with 50 to 249 employees amounted to 19% of all respondents from EU countries. All participants from the private sector can be split into two groups: separate companies and various business associations representing interests of different sectors (e.g. Internet and IT services, identification and trust services etc.).

The thematic analysis illustrated that respondents from the private sector emphasised six groups of challenges in the eIDAS implementation process:

- the fragmented legal framework and technical requirements;
- obstacles in mutual recognition and the interaction between the eIDAS-Nodes;
- the limited scope of the eIDAS network;
- security and privacy issues;
- excessive specialisation;
- and a different pace of digitization of the Member States

The most mentioned problems were connected to fragmentation in the legal framework (12 times) and technical requirements (22 times). Since these two themes are intertwined and difficult to split we considered them as one group. In the respondents' opinion, the legal framework needs to be more harmonised on the EU level because the national rules of the Member States stay fragmented and undeveloped. Such fragmentation leads to "a high level of uncertainty for businesses and effectively blocks consumers in some Member States". Besides the fragmented legislation, "the technology,

Table 1: Feedback by country of origin

Country	Number of Respondents	Weighted Percentage
France	12	22,64
Germany	7	13,21
Belgium	5	9,43
USA	5	9,43
Italy	4	7,55
Switzerland	3	5,66
Austria	2	3,77
The Netherlands	2	3,77
Czech Republic	1	1,89
Denmark	1	1,89
Estonia	1	1,89
Finland	1	1,89
Norway	1	1,89
Spain	1	1,89
Sweden	1	1,89
UK	1	1,89
N/A	5	9,43
Total	**53**	**100**

eID devices and protocols differ from Member State to Member State". There is also "a lack of common technical standards for digital identity matters". For instance, “the eIDAS does not establish certifiable standards for all digital identity providers”. The topic of remote identity proofing and its' lack of harmonization is the most mentioned in this group (11 times).

Approximately the same number of respondents from the private sector see obstacles in mutual recognition and eID schemes notification procedures (16 mentions), with the interaction between the eIDAS-Nodes (5) and in lack of relevant attributes (3). The category related to mutual recognition and eID schemes notification procedures includes the complexity of the notification process, incompatible requirements between policies, different interpretations of some articles of the regulation by national authorities.

Representatives from the non-EU countries would like the EU to collaborate on the international level and enable mutual recognition of the eID schemes. Moreover, two respondents draw attention to the fact that there is a lack of advisory institution on the EU level that is "advisory/administrative body to support the industry by implementing eIDAS". In addition, national “supervisory bodies have no legal enforcing authority”. Therefore, “a set of baselines of auditing rules and a baselines audit plan for each trust service” needs to be created. Two respondents brought out the need to cover management of emergencies (including back-up of eID schemes for emergency purposes).

There is also a need to amend the interaction between the eIDAS-Nodes (5 mentions). Identity matching is problematic as "some Member states do not have persistent identifiers", “no access requirements to exchange data between two eIDAS services”. Further, the lack of relevant attributes for several services was mentioned three times.

Another group of obstacles is relates to the limited scope of the eIDAS network and lack of demand and use cases, which was mentioned 21 times. Respondents found that "the current eIDAS framework is restricted to specific use-cases and is not a good fit for many solutions providing digital identity verification, particularly in the private sector”. The respondents propose that the framework could be extended to the private sector. Furthermore, more attention should be drawn to user experience and consumer preferences, including authentication processes.

From the security and privacy aspects (16), respondents found that there is a deficit of clarity about the eIDAS levels of assurance and too much interpretation room. Overall, the issue with the level of assurance was mentioned nine times. Some representatives suggested that the eIDAS regulation should be harmonized with the EU Cybersecurity Act and rely on General Data Protection Regulation [16]. 14 respondents from the private sector argued that some eIDAS norms are excessively specialized and, in some countries, local regulations are "restrictive and technology-specific". Consequently, the stakeholders warned that excessive regulation might lead to "rapid regulatory obsolescence" and restriction of innovation.

Respondents propose that eIDAS regulation should remain technologically neutral and used solutions must take into account the dynamic and evolving nature of the digital economy and the infrastructure (e.g. endorsing the OpenID Connect Standard besides SAML).

The different pace of digitization across the EU was mentioned three times (e.g. all Member States do not offer eID).

Regarding the EC's options for further eIDAS framework development (1. revise and slightly update the current regulation, 2. extend the effect of eIDAS to the private sector, 3. launch a European Digital Identity (EUid) or combine these three solutions), the preferences of private sector participants were split mainly between various combinations. 36% (11 respondents) of all private

[16] General Data Protection Regulation. Available: http://data.europa.eu/eli/reg/2016/679/oj

sector respondents, did not choose any option or combination of options. Overall, combinations between options 1, 2 and 3 and their combinations were equally popular.

5.2 Public Sector Feedback and Expectations

Seven representatives from the public sector organizations provided their feedback during the public consultation process (three from the national level, one from local, two from public academic institutions, and one from the postal service provider). Two of them represented French organizations, and others were from Spain, Italy, Estonia, the Netherlands and Finland. It would be better to explore the academic institutions' feedback separately, yet the small number of responses (two) does not allow generalizations. Therefore, public sector stakeholders' expectations also include an opinion of the research institutions.

Overall, the respondents from the public sector found the eIDAS regulation very valuable. However, at the same time, they point out that the legal regulation is not complete and does not cover all important areas, especially from the private sector perspective the whole potential of the regulation is not used.

Public sector representatives see the shift towards the attribute-based approach, but not towards the decentralized architectures, where the storage of attributes is under the direct (physical) control of users. The most frequently mentioned problems were related to the lack of standardization and control (was mentioned in 4 responses). Public sector representatives brought out following aspects regarding standardization:

- it is important to cover transactions between private parties;
- standardize the peer-review procedure;
- specify the minimum criteria relating to remote identification;
- determine the identification of devices and the Internet of Things procedures;
- organize training for citizens.

The revised version of the eIDAS regulation should create a legal grounds for allowing natural and legal persons to use a qualified electronic signature or seal. Some respondents argue that the trust services list should be further expanded or scope broadened (e.g. electronic archiving).

Alternatively, in others' opinion: "The introduction of digital identity trusted services, other than the eIDs already implemented under the eIDAS regulation, should not be pursued. As previously noted, if this were to happen it could undermine the massive efforts, organizational and economic, put in place by the Member States that have already developed notified digital identity systems."

There is also a lack of technological variations of the qualification mechanism or it is too specific. which may lead to the technological neutrality issue that was also brought out by other researchers [27].

When it comes to the three options proposed by the EC (1) revise and slightly update the current regulation, 2) extend the effect of eIDAS to the private sector, 3) launch a European Digital Identity (EUid) or combine these three solutions), respondent opinions were split between the first, second, and combined option. The respondents had different opinions about proposed options on the eIDAS development. Those favouring the first option, were concerned about additional financial costs and organizational changes of the already existing systems, which the second and third solution might cause. The public sector respondents did not show significant support for the third option due to financial considerations and respondents were afraid of setting up and managing parallel eID systems. They also saw a planned EUid as voluntary option. However, respondents found that the third option may be favourable for legal entities.

Public sector representatives supported the principle that notification of national eID schemes would be mandatory. The respondents were concerned about standardization and privacy related issues. People-centric approach was important for the public sector.

5.3 Third Sector, EU Citizens and Other Stakeholders Feedback and Expectations

The third group of respondents included 15 feedback: 10 from the EU Member States, two from non-EU countries (the USA and Switzerland) and three respondents with unavailable data. The most considerable number of responses in this group were from France (4), followed by respondents from Italy (3), Germany (2) and the Czech Republic (1). Five out of fifteen were NGOs from the identification, trust services and research domains, five EU citizens, one from council of notaries and four respondents preferred to remain anonymous.

The thematic analysis reflected four main challenges in the eIDAS implementation process. This includes the first group with fragmented technical requirements and legal framework, the second group with eIDs mutual recognition and lack of relevant attributes, the third group about the limited scope of use cases and finally security and privacy issues. Challenges from the last two groups were mentioned once in each case.

The most mentioned issue was technical requirements fragmentation (8). Respondents found that more strategic directions are needed for leveraging the benefits for the end-users and the system.Respondents expected the European Standard Organizations to complete the current set of eIDAS. They also emphasised that over regulations should be avoided.

The limited scope of the eIDAS framework was mentioned seven times. As a solution they proposed to stimulate the market and create new trust services and extend the regulation over the private sector entities. Some non-EU participants from this group reminded to consider the cases where EU citizens need to use electronic identities outside of the EU and extend interoperability to the international partners.

Security and privacy topics are essential for this group (5 mentions). For instance, some respondents concerned about private trust service providers, who might not guarantee sufficient personal data security if there are no specific rules and standards to follow.

Lack of relevant attributes was mentioned six times, while obstacles in mutual recognition – three times. Some respondents believed that "the notification process at European level shall remain a prerogative". Respondents proposed harmonisation of legal entity datasets and harmonise the identities of professionals using Legal Entity Identifier (LEI) that enables to link persons, companies and devices.

Almost half of the respondents of this group preferred to notify the EC about their concerns on further eIDAS framework development and not to choose between options proposed by EC.

6 DISCUSSION

Based on the research results it is possible to analyse the EC's European Digital Identity framework proposal and different stakeholders' expectations towards it. Stakeholders see various challenges in the eIDAS implementation and many of them are similar. Among mentioned obstacles are fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure and excessive specialization. Those perceived shortcomings correspond with the previous research results that indicated "compliance issues", "interpretation problems", "different practices in member states" and "representation of legal person challenges"[12].

If we analyse the EC's proposal, it is possible to say that the EC has covered many of the stakeholders' expectations. For example, widening the current eIDAS regulation scope in terms of new trust services, harmonizing the regulation with other EU regulations and standards, focusing on the cross-border service provision inside the EU and clarifying sharing of different electronic attributes.

However, there are some important topics that EC proposal does not address brought out by stakeholders. It has to be noted, that the stakeholders emphasized the need of technology neutrality and they did not prefer the option to launch a European Digital Identity (EUid). The EU digital identity wallet proposal seems to be further development of the initially proposed EUid solution, that enables additional benefits for the users (e.g. attribute sharing, qualified digital signature etc.). Stakeholders also expect solution to the legal entities representation issue that the EU digital identity wallet should solve.

It is questionable if the EC proposal should cover standardized e-service provision across the EU borders with third countries. However, the stakeholders are interested about this topic and would like it to be clarified. The EC proposal does not pay much attention to the notification of the national eID schemes mentioned by the stakeholders. However, the notification process does not have to be regulated on the legal act level and can be specified in other regulatory documents.

Security and privacy issues are not directly reflected in the proposal. However, it is possible to take these aspects into account while designing the technical architecture of the EU digital identity wallet and specifying applicable technical standards. Stakeholders also warn against over regulation and standardization that may also happen during the legislative process.

7 RESEARCH LIMITATIONS AND FUTURE DIRECTIONS

Every research has some limitations. For example if it comes to the stakeholders, then the private sector view was more strongly presented than public sector opinion. Further, it is possible to notice that France was very much engaged in the consultation with the most significant share of all participants. The probable explanation of such interest was that France was preparing to pre-notify its eID scheme under the eIDAS regulation at that time, which resonated through a high participation rate in the consultation process.

On the other hand, the low number of respondents from the public sector and citizens' representatives limit the possibilities to generalize enough the research results of this sector. Moreover, the results reflect only opinions of those, who provided their feedback on the eIDAS public consultation process. We also could only analyse the opinions that were published on the EC website.

Future research perspective should cover analysing the final outcome of the EU Digital Identity Framework regulation. Also, it is possible to evaluate some of the stakeholders expectations after the EC and the Member States have agreed the technical details of the EU digital identity wallet solution.

8 CONCLUSION

The eIDAS revision is a part of the EU strategy, because the EU Digital Single Market largely depends on its enablers: eIDs and electronic trust services. To ensure a high usability of eIDs and to correspond to the users needs, it is important to take into account the feedback of different stakeholders in the eIDAS revision process.

This research focused on the public and private sector stakeholders' feedback analysis provided during the eIDAS public consultation procedure initiated by the EC. We compared the stakeholders feedback with the EC eIDAS amendment proposal and establishing a framework for a European Digital Identity. The aim was to identify if the stakeholders expectations were covered and to contribute to the ongoing eIDAS revision process. Stakeholders mentioned following challenges regarding the eIDAS regulation: fragmented technical requirements and legal framework, the limited scope of eIDAS and use cases, security and privacy issues, the complexity of the notification procedure and excessive specialisation.

Research results indicate that the majority of the stakeholders' expectations are covered by the EC proposal. However, many aspects and their correspondence to the stakeholders' needs depend on the final technical, architectural and procedural agreements between the EC and the Member States. On the stakeholder level, there are some eID related topics that need EU level solutions, but are left out of the EC's proposal. Discussions concerning the EC's proposal are ongoing and final evaluation can be done once the final regulation draft is accepted.

REFERENCES

[1] Gerli Aavik and Robert Krimmer. 2016. Integrating digital migrants: Solutions for cross-border identification from e-residency to eIDAS. A case study from Estonia. In *International Conference on Electronic Government*. Springer, 151–163.
[2] Ali M Al-Khouri. 2014. Digital identity: Transforming GCC economies. *Innovation* 16, 2 (2014), 184–194.
[3] Álvaro Alonso, Alejandro Pozo, Aldo Gordillo, Sonsoles López-Pernas, Andrés Munoz-Arcentales, Lourdes Marco, and Enrique Barra. 2020. Enhancing University Services by Extending the eIDAS European Specification with Academic Attributes. *Sustainability* 12, 3 (2020), 770.
[4] James Backhouse. 2006. Interoperability of identity and identity management systems. *Datenschutz und Datensicherheit-DuD* 30, 9 (2006), 568–570.
[5] Diana Berbecaru, Antonio Lioy, and Cesare Cameroni. 2019. Electronic identification for universities: Building cross-border services based on the eIDAS infrastructure. *Information* 10, 6 (2019), 210.
[6] Konstantinos Gerakos, Michael Maliappis, Constantina Costopoulou, and Maria Ntaliani. 2017. Electronic authentication for university transactions using eIDAS. In *International Conference on e-Democracy*. Springer, 187–195.
[7] Anssi Hoikkanen, Margherita Bacigalupo, Wainer Lusoli, Ioannis Maghiros, and Stavri Nikolov. 2010. Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies. In *IFIP Working Conference on Policies and*

Research in Identity Management. Springer, 41–58.
[8] Armen Khatchatourov, Maryline Laurent, and Claire Levallois-Barth. 2015. Privacy in digital identity systems: models, assessment, and user adoption. In *International Conference on Electronic Government*. Springer, 273–290.
[9] Tomaž Klobučar. 2019. Facilitating Access to Cross-Border Learning Services and Environments with eIDAS. In *International Conference on Human-Computer Interaction*. Springer, 329–342.
[10] Herbert Kubicek and Torsten Noack. 2010. Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society* 3, 1 (2010), 235–245.
[11] Mirosław Kutyłowski, Lucjan Hanzlik, and Kamil Kluczniak. 2016. Pseudonymous signature on eIDAS token–implementation based privacy threats. In *Australasian Conference on Information Security and Privacy*. Springer, 467–477.
[12] Silvia Lips, Nitesh Bharosa, and Dirk Draheim. 2020. eIDAS implementation challenges: the case of Estonia and the Netherlands. In *International Conference on Electronic Governance and Open Society: Challenges in Eurasia*. Springer, 75–89.
[13] Frank Morgner, Paul Bastian, and Marc Fischlin. 2016. Attribute-based access control architectures with the eIDAS protocols. In *International Conference on Research in Security Standardisation*. Springer, 205–226.
[14] Frank Morgner, Paul Bastian, and Marc Fischlin. 2016. Securing transactions with the eIDAS protocols. In *IFIP International Conference on Information Security Theory and Practice*. Springer, 3–18.
[15] Thomas Neubauer and Johannes Heurix. 2010. A roadmap for personal identity management. In *2010 Fifth International Conference on Systems*. IEEE, 134–139.
[16] Kim Nguyen. 2018. Certification of eIDAS trust services and new global transparency trends. *Datenschutz und Datensicherheit-DuD* 42, 7 (2018), 424–428.
[17] RM Pelikánová, Eva Daniela Cvik, Robert MacGregor, et al. 2019. Qualified electronic signature–eIDAS striking czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis* 67, 6 (2019), 1551–1560.
[18] Paul P Polanski. 2015. Towards the single digital market for e-identification and trust services. *Computer law & security review* 31, 6 (2015), 773–781.
[19] Carlos Ribeiro, Herbert Leitold, Simon Esposito, and David Mitzam. 2018. STORK: a real, heterogeneous, large-scale eID management system. *International Journal of Information Security* 17, 5 (2018), 569–585.
[20] Floris Roelofs, Eric Verheul, and Bart Jacobs. 2019. *Analysis and comparison of identification and authentication systems under the eIDAS regulation*. Ph.D. Dissertation. Master's thesis, Radboud University, the Netherlands.
[21] Paolo Smiraglia, Marco De Benedictis, Andrea Atzeni, Antonio Lioy, and Massimiliano Pucciarelli. 2017. The FICEP Infrastructure. In *International Conference on e-Democracy*. Springer, 196–210.
[22] 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*. 340–341.
[23] Valentyna Tsap, Ingrid Pappel, and Dirk Draheim. 2019. Factors affecting e-ID public acceptance: a literature review. In *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 176–188.
[24] Muhamed Turkanović and Blaž Podgorelec. 2020. Signing Blockchain Transactions Using Qualified Certificates. *IEEE Internet Computing* 24, 6 (2020), 37–43.
[25] Astrid Valtna-Dvořák, Silvia Lips, Valentyna Tsap, Rain Ottis, Jaan Priisalu, and Dirk Draheim. 2021. Vulnerability of State-Provided Electronic Identification: The Case of ROCA in Estonia. In *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 73–85.
[26] José van Dijck and Bart Jacobs. 2020. Electronic identity services as sociotechnical and political-economic constructs. *new media & society* 22, 5 (2020), 896–914.
[27] Anne Veerpalu, Liisi Jürgen, Eduardo da Cruz Rodrigues e Silva, and Alex Norta. 2020. The hybrid smart contract agreement challenge to European electronic signature regulation. *International Journal of Law and Information Technology* 28, 1 (2020), 39–84.
[28] Robert K Yin. 2018. *Case study research and applications*. Sage.

Appendix 3

III

S. Lips, R. K. Ahmed, K. Zulfigarzada, R. Krimmer, and D. Draheim. Digital sovereignty and participation in an autocratic state: Designing an e-petition system for developing countries. In *the 22nd Annual International Conference on Digital Government Research*, dg.o 21, page 123–131, New York, NY, USA, 2021. Association for Computing Machinery

Digital Sovereignty and Participation in an Autocratic State: Designing an e-Petition System for Developing Countries

Silvia Lips
silvia.lips@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

Rozha K. Ahmed
rozha.ahmed@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

Khayyam Zulfigarzada
khayyam.zulfigarzada@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

Robert Krimmer
robert.krimmer@ut.ee
Johan Skytte Institute of Political Studies, University of Tartu
Tartu, Estonia

Dirk Draheim
dirk.draheim@taltech.ee
Information Systems Group, Tallinn University of Technology
Tallinn, Estonia

ABSTRACT

Establishing a sustainable citizens-government dialogue is a crucial topic on the agenda of many countries. E-petition systems are among the most popular and effective tools for establishing a responsive and effective dialog between governments and citizens. E-petition systems mitigate the gap between citizens and government authorities and contribute to the empowerment of citizens. This study aims to determine how to increase citizens' participation in decision-making processes through the case of an e-petition system in Azerbaijan. The research employs a mixed method of qualitative and quantitative data collection methods within a case study design. Data were collected from a triangulation of multiple sources, i.e., interviews with state authorities and online survey among the citizens of Azerbaijan. Additionally, we reviewed experiences from other countries that introduced e-petition systems, in order to better understand the success factors of and obstacles to launching e-petition systems, with a particular focus on the needs of developing countries. The outcome of this study is a proposed design of an e-petition system model that can be considered in developing countries.

CCS CONCEPTS

• **Information systems** → *Computing platforms.*

KEYWORDS

e-petition, e-participation, e-democracy, citizens empowerment

ACM Reference Format:
Silvia Lips, Rozha K. Ahmed, Khayyam Zulfigarzada, Robert Krimmer, and Dirk Draheim. 2021. Digital Sovereignty and Participation in an Autocratic State: Designing an e-Petition System for Developing Countries. In *DG.O2021: The 22nd Annual International Conference on Digital Government Research (DG.O'21), June 09–11, 2021, Omaha, NE, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3463677.3463706

DG.O'21, June 09–11, 2021, Omaha, NE, USA

ACM ISBN 978-1-4503-8492-6/21/06.
https://doi.org/10.1145/3463677.3463706

1 INTRODUCTION

In a number of countries around the world, regardless of the social and economic conditions, public dissatisfaction is one of the fast-growing internal problems [6, 7]. In some societies, the level of public dissatisfaction reaches a worrying level and very often leads to significant consequences [6, 15]. Citizens are disgruntled with the quality of work of state and regional government authorities that can result into distrust [20].

Citizens may become frustrated, when their complaints and appeals do not reach relevant authorities, i.e., if we encounter a lack of official and effective communication between the government and its citizens or lack of motivation from the authorities side to meet citizens expectations [8]. Too often, citizens' request for support and attention remain unheeded. In a society where the government keeps itself away from its citizens, and where citizens cannot interact with the officials at an appropriate level, an atmosphere of hopelessness and mistrust to the government can emerge. Gradually, people become reluctant to participate in decision-making processes, as they loose interest and do not see themselves as stakeholders who can influence state decisions.

Unfortunately, very often in developing countries there is an insufficient level of communication between the state and its citizens. In the case of Azerbaijan, studies have shown that most of the population of Azerbaijan is dissatisfied with the current level of dialogue and is experiencing problems to express their opinion to the relevant state structures and authorities[1] [1]. Although the Azerbaijan government is enormously interested in raising e-government technologies in the country, which shows, e.g., in the establishment of an "E-government Development Center" [23, 27]. However, in 2018, the problem of lack of dialog between citizens and government in Azerbaijan still exists. Such problems are plausible, as it is known from research of authors like Gustav Lidén, that autocratic countries regularly achieve lower scores in e-participation and e-democracy than countries that are more democratic [17], p. 706*ff.*

[1] Bertelsmann Stiftung's Transformation Index (BTI) 2018. Available: https://www.ecoi.net/en/file/local/1427383/488339_en.pdf

Considering these aspects, this research aims to propose and design an e-petition system for developing countries using Azerbaijan as a case study. The main research question is the following:

- How to design an e-petition system for developing countries enabling additional channel for citizen's participation in public decision making?

It is important to consider relevant vital social, political and technical conditions in the country. Regarding the methodology, this research employed a case study design through a mixed approach of qualitative and quantitative data collection methods. The authors analyzed the current environment in the country and whether the country is able to ensure the preconditions for successfully implementing an e-petition system. We used different sources for data collection. From this analysis, it turned out that a major success factor is in the government authorities' interest into and usage of the system. The authors conducted several interviews with public officials from different Azerbaijani authorities. Moreover, citizen views were considered as significant measure through an online survey.

Sect. 2 provides an overview of relevant efforts on e-petition systems in other couturiers. Sect. 3 presents the research methodology, together with an overview of the case of Azerbaijan, and data collection procedure. Sect. 4 presents the findings of the analysis. Then, Sect. 5 proposes an e-petition system model for Azerbaijan. Sect. 6 presents limitations and future direction of the study. The paper finishes with a conclusion in Sect. 7.

2 LITERATURE REVIEW

Several countries in the world already benefit from the implementation of e-petition platforms [10]. Positive experiences of those countries have shown that with a smart and comprehensive approach, such tools can yield very good results [9].

The main goal of this research is to propose a suitable e-petition system model for developing countries that can help to increase citizens' participation and engagement in the decision-making process. Undoubtedly, in service of this case, international experience should be considered and studied. It is important to use the experience of other countries to understand what aspects contribute to the successful functioning of e-petition platforms, which obstacles might interfere with them and how to overcome those [5]. In this section, the authors focus on the most important structural parts and different examples (both successful and unsuccessful) in order to understand how to build a model that will be suitable for Azerbaijan and could be used also in other developing countries [9].

For example, Ukraine has introduced a de-centralized web-based platform through which petitions can be signed. All petitions that collect more than 25,000 signatures within 3 months are be discussed by the government authorities [14]. However, the e-petition platform is not very popular and the Ukrainian Parliament's petitions are practically not functional [21].

Similarly, Moldova implemented a web-based centralized environment where petitions are submitted via the government web-site and signed using e-signatures[14]. The e-participation in Moldova is low and political context for e-petition activities rather unfavorable. There is lack of trust towards the authorities and low technological awareness. Instead of using e-petition environment provided by government, the enthusiasts prefer organising separate campaigns [13].

The United Kingdom also implemented a web-based centralized environment where British citizens or UK residents can initiate petitions and government respond to petitions that get at least 10,000 signatures[19][2].The example of UK can be considered as successful as, since 2015, electronic petitions in UK collected a total of 50 million signatures; and the process of signing petitions has become the second most popular form of political activity after voting[4].

In Estonia, several web-based e-petition platforms exits that allow for proposing ideas and collecting signatures in support of proposed ideas, for expressing opinions on legal drafts, as well as for searching legal acts and strategies. One of these examples is web-based e-petition platform osale.ee [3]. However, this particular example in the field of e-petition field cannot be considered as successful [24].

The United States (US) e-petition system is considered practical as compared to other web-based application systems in the country. In the system, it is possible to continue collecting signatures after submitting a petition to the governmental authorities[3]. In 2005, the German federal parliament (Deutscher Bundestag) launched an online e-petition platform, that allows for signing petitions and to discuss them in a forum[22]. According to [18], the German system is dominated by small number of high-volume petitions[11] and petitioners belong to the younger generation. In addition, it is important to mention that among the younger generation, different social media platforms play significant role in terms of sociopolitical engagement[2].

The success of e-petition systems has been influenced by many aspects specific to each of the several different countries such as technical equipment of the country, technology awareness of the people, the level of education, cultural and historical background, whether the concept of e-petition is familiar to the public etc. [10] The authors tried to focus not only on examples of developed western countries but also on the experience of countries that have a cultural background and level of development that are more similar to those of Azerbaijan.

Based on the literature review, it is possible to say that there is no single model suitable for immediate adoption in developing countries. However, it is possible to use elements and practice from previously described countries to design an e-petition system model more suitable for developing countries.

3 RESEARCH APPROACH

This research adopted a case study strategy, as it conducts an in-depth investigation of a contemporary phenomenon within its real-life context [25]. A case study is suited when the boundaries between a phenomenon and a context are not completely clear, and whenever there is a lack of earlier studies to estimate the outcome. Considering that, this strategy is well-suited for the case of Azerbaijan to investigate the current state and present a sustainable

[2]https://petition.parliament.uk/
[3]www.osale.ee

and effective model of e-petition system as a first engagement platform between citizen and government in Azerbaijan.

3.1 The Case of Azerbaijan

Azerbaijan is located in the crossroads between Eastern Europe and Western Asia. Being a former soviet and developing country, Azerbaijan tries not to stay behind in a sphere of technological development, including the e-government sector. The country has successfully implemented several e-government projects and keeps showing rising interest in this field [26].

Currently, Azerbaijan faces the problem of a lack of a dialog between its citizens and the government. Even though the Azerbaijani government shows interest in e-government, yet, no e-democracy projects have been launched in the country.

It is clear that before launching a similar system in Azerbaijan, the government should have a clear vision of how to implement it correctly. It is important to consider all vital social, political and technical conditions in the country to ensure all necessary conditions for making the system successful. Such tool as e-petition system can help to solve a number of problems related to citizen participation in decision making process for the case of Azerbaijan.

3.2 Data Collection

Given the nature the research, it was decided to use mixed of qualitative and quantitative data collection methods. Investigating the problem of proposing a successful e-petition system model, requires a complex and comprehensive approach and therefore using both qualitative and quantitative data collection methods helps to get a better overview and understanding of the issue. Supported by reviewing existing relevant literature.

Considering that the ultimate goal of the research is to find an answer about how to design the most suitable e-petition system for developing countries similar to Azerbaijan, the source and process of data collection for the research can be divided into three groups.

3.2.1 Qualitative Method – Interviews. The state agencies play a significant role in the successful implementation of e-petition systems, as they cannot function without proper support of state structures. Regarding the attitude of state structures towards launching such platform, the authors conducted four interviews with official representatives of government bodies of various fields. The interviewees were chosen according to the sector of their organization. The authors focused mainly on sectors that interact with the citizens on a regular basis and provide services that have a crucial influence on the daily life of citizens: public transportation, education, social protection, and finance. All interviewees were informed about the purpose of the interview and the overall research processes. The interview were composed of 12 questions.

The interviewees have been:

- The Head of the Sumgayit Transport Agency under the Sumgayit city executive power from The Public transportation services.
- The deputy head of the Regional Financial Settlement Center No. 1 under the Ministry of Education.
- The leading adviser of the social service sector from the Absheron regional branch of the Ministry of Labor and Social Protection of Population.
- The leading Specialist from the ortgage and Credit Guarantee Fund of the Republic of Azerbaijan.

3.2.2 Quantitative Method – Online Survey. Considering the specifics and nature of this kind of systems there is a need to understand the citizens' view and expectations towards the e-petition system. A mass online survey is a fast and affordable way of collecting data and covering a broad number of respondents. The target group of the survey have been citizens of Azerbaijan, no matter of the social status, occupation, gender, and other aspects, as the system aims to be equally accessible for citizens. The survey has been conducted through the internet and spread among the population via social media channels. As already reflected from the literature review, technological awareness is one of the pre-conditions of the successful implementation of the e-petition system. Therefore, people who are already able to participate in the online survey, provide valuable input of their expectations towards the e-petition system being at the same time potential users in future.

264 citizens took part in the survey. The survey was composed out of 15 questions. Questionnaire was divided into three parts. The questions in the first part mainly aimed to clarify the purpose, frequency, and level of internet use among the participants. In the second part of the survey requesting sharing participants experience on the current situation of the dialogue between citizens and the government and their personal views and expectations about e-petition portal. The third part related to the model and functionality of the system to understand the preferences of potential users.

3.2.3 Document Analysis. Another significant source of data is positive as well as negative examples and experience of other countries that have already launched an e-petition platform. Therefore, we analysed different data sources (reports, scientific literature etc.) of different countries. In Estonian case we even contacted osale.ee team to receive written feedback from the system implementation. It is crucial to analyse different documentary sources to understand what aspects affect successful functioning of e-petition platforms, which obstacles might interfere and how to overcome them. International experience is also valuable especially considering the fact that this research is new for Azerbaijan and there are no materials related to e-participation tools in the particular country context.

Figure 1 presents the current research approach and data sources.

3.3 Validity Check

The four criteria of validity judgment such as, *construct validity*, *internal validity*, *external validity*, and *reliability* in [25], were considered as an essential part of the study to assure the quality of research design.

- *Construct validity* is achieved through using a triangulation of multiple data sources such as interview, survey and document analysis to strengthen the validity of the information.
- *Internal validity* is more concerned with finding the causal relationship between outcomes and treatment [25]. As this current case study research is limited to only investigate the state and propose an effective model, it might be possible in further studies to explore the causal relationship.
- *External validity* is to ensure the generalization of the results. Authors provided detailed procedure of the research.

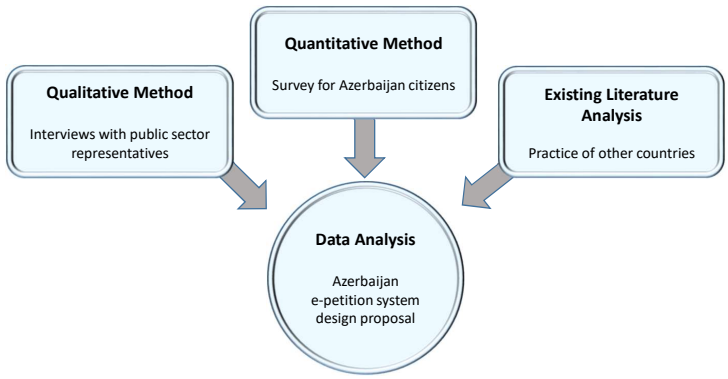

Figure 1: Research approach and data sources

Literature review and later document analysis showed that autocratic states face similar challenges with regards the e-petition systems. Therefore authors believe that the result can be generalized by producing the same process, in specific, for developing couturiers with a similar environment as Azerbaijan.

- *Reliability* is relevant to the ability of replicating the same procedure by different researchers and producing the same results. To ensure reliability of the research, authors created a case study protocol and documented all the procedures in the database.

4 FINDINGS

This section describes outcomes of the interviews and online survey. Based on this data it is possible to design and propose the most suitable and effective e-petition model for Azerbaijan that could be applicable also in other developing countries.

4.1 Interview Results

Four Azerbaijani state authorities were interviewed in order to understand their attitude towards the idea of implementing an e-petition system in Azerbaijan. It was important to understand whether they support the idea and would be ready to cooperate if the platform will be implemented.

The first two questions of the interviews were related to the functionality of the state organizations where interviewees were working and what services their orgnizations provide to the citizens. Interviewees described briefly the functionalities and roles of those bodies and also described the type and delivery-process of the services. Interviewees were also asked to evaluate the level of communication with the citizens in their organization. All respondents stated that the level of communication with citizens is at a very good level. Only one interviewee noted that he would prefer to increase the scale and audience of communication with citizens. The interviewee declared that at the moment, communication is mainly based on the requests from individuals, but the nature of the service that they provide requires in his opinion communication at the level of large groups of people since the requests are identical in most of the cases. Grouped requests would facilitate the work and save resources of the organisation. Interviewees noted that currently they use hot-lines and e-mails as communication channels with the citizens and they are always open for the appointments. One interviewee stated that they use electronic platform to communicate within the ministry with the other agencies under the jurisdiction of the same ministry as well as receive requests from the citizens and respond to them. All respondents stated that they consider these channels to be quite effective, but at the same time, they would not mind any improvements and the introduction of new ones.

Regarding the availability, feedback mechanism which could measure whether the citizens are satisfied with the service they provide, two interviewees admitted that they do not have any feedback mechanism. The rest two interviewees claimed that they call the customers after solving their issue and ask whether they were satisfied by the provided service or not. All respondents agree with the statement that high-quality communication favorably affects the quality of work of the organization and its reputation in the society. Moreover, one of the respondents even said that a good quality dialogue with citizens will give them a sense of security and strengthen their trust towards the government. This issue, in turn, depends also on the allocation of funds for this organization from the state budget.

Three out of four respondents had information on the experience of countries that have implemented electronic participation and e-petition portals. All four interviewees declared that they would like to have similar system implemented in Azerbaijan.

Respondents brought out following benefits with regards to the e-petition platform:

- The e-petition system helps to identify the most acute and important problems in the society and therefore authorities primarily can focus on the most urgent ones.

- The e-petition system helps citizens to inform authorities about their problems and establishes two-way communication between the citizens and authorities.People often prefer to complain to each other rather than to forward their complaints to the appropriate authority. This, in turn, harms the organization's reputation, without even giving it a chance to find out about the problem and try to solve it.
- The e-petition platform can also be used for legislative discussions and for conducting mass surveys among the population. This option would be very beneficial for government organizations in terms of cost-saving.
- A large number of signatures collected via e-petition system indicates clearly the seriousness of a problem in the society. If an organization needs additional funding, the process of requesting funds from the state budget will be much easier.
- The existence of such system can lead to the strengthening of civil society in a country. Citizens will more actively take part in the decision-making process. They understand better their importance and responsibility in these processes.

Finally, all respondents expressed their support and interest towards the idea and stated that if such system will be launched in Azerbaijan they would definitely use it. Interviewees also expressed their advice and recommendations regarding how they would like to see the e-petition platform. Two of them recommended that there should be a certain working group that would check the feasibility of the petitions before sending them to the appropriate authority, as well as distribute the petitions to the relevant state bodies as citizens can experience difficulties by doing it themselves. One interviewee suggested that petitions with a large number of votes should be discussed in the parliament. Based on the interviews it is possible to bring out following key findings:

- Government officials in Azerbaijan are aware of the phenomenon of electronic petitions. They have an understanding how the e-petition system is functioning and what benefits and values it can bring to the country.
- Officials consider the current level of dialog and quality of communication channels satisfactory. But at the same time, they accept that the platform of e-petitions would certainly be able to take the dialogue to a new level.
- Government officials are tech-savvy enough to collaborate with the e-petition portal, as they already use special software and internal e-portals on their workflows.
- There is a lack of feedback mechanism. In most cases, state authorities do not receive any feedback from the society regarding the service(s) they provide.
- Government officials are very enthusiastic regarding the idea of implementing such system in the country. They are open for cooperation.

4.2 Survey Results

A web-based survey was conduced for understanding citizen's attitude regarding the potential e-petition system. As the survey was spread through the Internet, only people who had an access to the Internet could express their opinion. Therefore, the survey does not cover the full spectrum of the population. However, at the same time, it is obvious that only people with an Internet access are able to take part of different ICT initiatives.

The survey was actively promoted and open for participation during a period of 3 weeks. During this period 264 respondents took part of the survey. Respondents were asked 15 questions and it was possible to share their own views or suggestions regarding the e-petition system. The survey was divided into 3 parts: general information about the respondent, respondent's views on the current situation of the dialogue between citizens and the government and his/her personal views and expectations towards the e-petition system.

78.4% of the respondents were 18-29 years old, 17,8% 30-45 years old and respondents under 18 together with respondents 46 and up accounted for 3,8% of the total amount of respondents.

Rather high percentage (45.8%) of the respondents had enough skills for using such comparatively complex e-services such as e-banking and e-shopping. 27.3% of the respondents outlined that they work in digital space, therefore they can use the Internet on a professional level. 24.2% responded that their skills are limited to finding information they need.

Survey respondents indicated that they use the Internet usually to find some information, for entertainment and for the communication purposes. 50% percent of the respondents said that they often use the Internet to pay utility bills, taxes etc. To the question if they ever heard or used any public e-services before, 46.6% respondents answered "yes, but not on regular basis" and 21.2% said that they use regularly e-services that exist in the country. At the same time 21.2% responded that they are aware of the e-services but have never used them before. 11% of respondents claimed that they have never heard about such services and therefore have not used any public e-services.

Most citizens believe that responsiveness of the government depends on how big is the problem for the society. Almost 30% of the respondents claimed that there is no dialogue between the government and citizens at all. 6.8% of the respondents did not know how to contact with the government authorities. Only 18.2% of citizens believe that the citizens-government dialogue is on a good level and government bodies respond to the citizens' requests.

Most respondents said that they use the hot-lines of the ministries as the main channel to communicate with them. The second most popular method according to the respondents is sending e-mails and applications through the official websites of the authorities. 12.5% of citizens have not even tried to contact the authorities, as their previous experience has shown that this is completely useless. Almost the same percentage of citizens declared that they always try to get an appointment and meet the officials. The left 20% of the respondents have never tried to contact the officials, as they have not had any necessity for this.

Slightly more than half of the respondents said that if e-petition platform will be launched in Azerbaijan, they will definitely use it. 37.9% said that they will use it only if somebody explains how to use it, first. Only 8% were skeptical and said that they would not use the e-petition platform since they do not believe in its effectiveness.

Citizens of Azerbaijan are aware of the existence of electronic petitions as a phenomenon. Some respondents even indicated that they

had previously signed petitions on a platform such as Change.org, which is quite popular in Azerbaijan. Only one-third of respondents admitted that they have never heard about such platforms before. More than half of the respondents have optimistic views on the system and believe that it can solve number of problems and take citizen-government dialogue to the next level. 16% of respondents are skeptical and do not find implementing an e-petition system as a good idea and 10% think that the system will not receive a proper level of support and cooperation from the authorities.

In order to follow the new petitions, citizens would like the e-petition portal to have its own pages in social network(s). In their opinion, it will be easier to stay informed about the petitions and also share them with friends. Many respondents supported the idea of sending the most popular and fast-growing petitions to their e-mail addresses.

Regarding the issue of registration and authorization procedure, most citizens said that they would like to open a personal account in the e-petition platform. They do not mind sharing necessary data for this. A little more than 30% percent of respondents would like to use their mobile ID for this. When citizens were asked whether they want their name to be displayed under the signed petitions, 56% percent of the respondents did not see any problem in that. 35.2% of the respondents wanted to have a function that allows them to decide whether to display their name or not. Only 9.8% of the respondents preferred to remain anonymous.

Respondents supported the idea of publishing state readings, government documents and other related information on the e-petition platform. Citizens also showed a positive attitude towards the participation in legislation draft discussions or in mass surveys conducted by the government bodies.

The survey showed that if the e-petition platform will be launched in Azerbaijan, citizens will show interest and support it. Internet users would be capable enough to use such kind of platform as most of them already use periodically e-government and other electronic services. Survey results concluded recommendations from the respondents how they would like to see the e-petition platform from the design and functionality perspective.

5 DISCUSSION

Findings presented that citizens and government officials show quite positive attitude towards the idea of launching an electronic petition system in the country. The vast majority of the survey participants had very optimistic views and expectations towards the e-petition system. An interesting detail was that despite the fact that the majority of the population declares that the level of dialogue with government bodies is low, government officials believe that the dialogue between their authorities and the population is on a fairly good level. At the same time, it should be noted that government officials accept the need for improvement and expansion of current communication channels.

Azerbaijan has the competence and experienced people to implement this kind of system and related public e-services. State authorities and institutions are sufficiently equipped with ICT infrastructure and use Internet technologies on a daily basis as a vital part of their workflows. Government officials are tech-savvy, experienced, and trained enough to use different ICT tools necessary for the e-petition system implementation.

Regarding the digital literacy and readiness of the population, according to the international reports, it is at a satisfactory level [12, 16, 26]. Most of the population is actively using the Internet, including public e-services and a number of other digital services. Regarding the country's technical readiness for introducing an electronic petition system, report outcomes from relevant international organizations are also quite positive[4].

Despite the existing difference in the Internet usage and digital literacy between urban and rural populations, the country's technical capabilities are satisfactory for introducing this type of system in Azerbaijan [26]. Such a difference been rural regions and cities is typical not only for Azerbaijan but also for most countries in the world.

5.1 e-Petition Design Proposal

Existing literature analysis and suggestions from the interviewed state officials clearly showed that an e-petition committee is a necessary part of a well functioning e-petition system. The Committee plays a role of an intermediary body that coordinates the interaction of the citizens with the relevant state bodies through the e-petition platform. The Azerbaijani e-petition committee may comprise of members of the parliament, similar to the German model. But authors believe, that it may also be controlled by a separate body such as the E-Gov Development Center of Azerbaijan republic [5]. The reason for this is the presence of specialists who are more likely aware of the functioning principles of such systems. In addition, it is important to examine and correct periodically existing errors in different functionalities of the e-petition platform. The most competent authority capable of doing this is "E-Gov Development Center". Therefore, it would be reasonable if the work of the committee, as well as the research and technical works related to the system, would be carried out by that institution. Authors believe that at the initial stage of the e-petition system implementation the petitions should be sent only to the state authorities. Based on the existing literature and practice analysis, in some of the countries petitions are discussed on a parliamentary level after collecting high number of signatures. Authors do not consider such model viable for Azerbaijan, at least not in the initial phase because it slows down the system implementation speed.

The main operations of the e-petition system considered for Azerbaijan are presented as follows.

- **Account creation/authorisation.** In order to sign the petition the user should create an account by providing following data: full name, phone number, e-mail address, physical address, personal identification code and postcode.
- **Creation of the petition.** The applicant should choose laconic and attractive name for the petition in order to engage more people. Then a wide description of the petition should be entered using well understandable language. It is important to indicate clearly the problems, explain the proposal,

[4]United Nations e-Government Survey 2020.
[5]E-Gov Development Center. Available: https://www.digital.gov.az/en

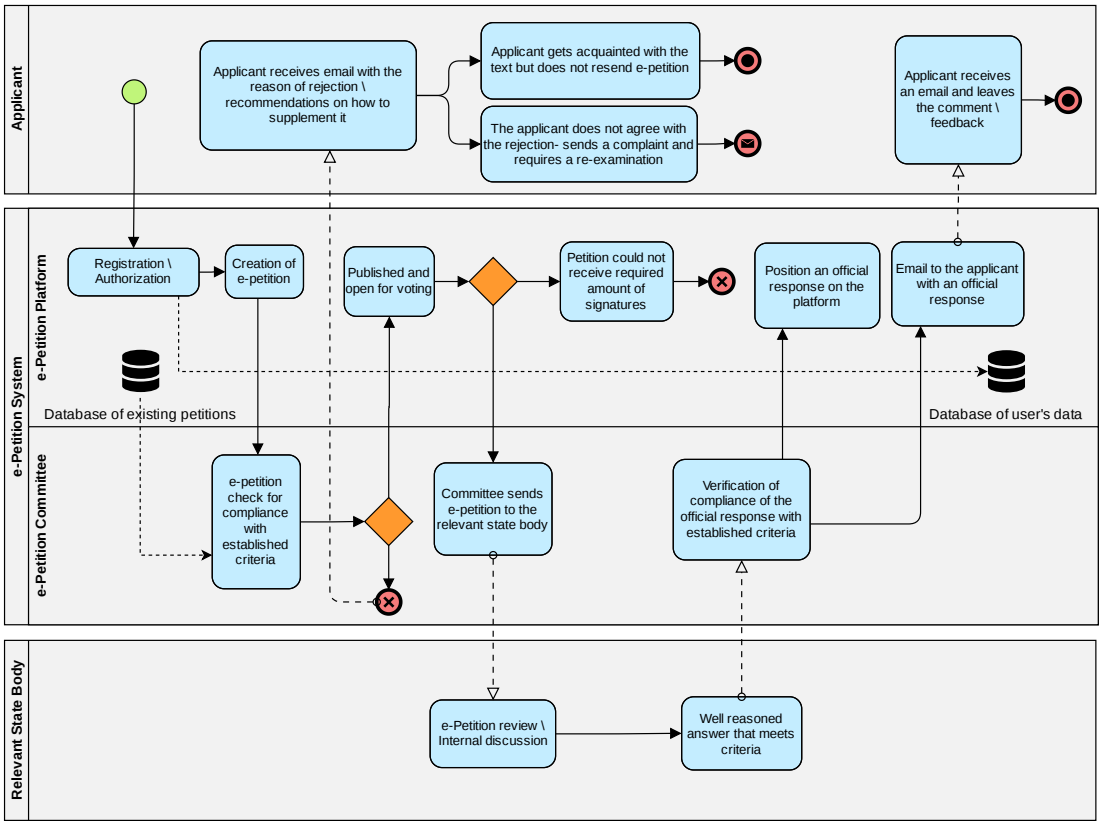

Figure 2: Proposed e-petition model

and what the applicant expects from the state authority. The reference data attached to the petition is welcome.

- **Proceeding the e-petition.** Compliance of the submitted e-petition and also the absence of identical petitions in the system is checked. After that, the petition is put to a universal vote for a 2 month period. The form of the published e-petition reflects following information: full name of the applicant, the petition text, the classification of the topic, reference materials and the number of signatories. Under the e-petition form, from the moment of its publication, a forum opens where citizens can discuss the petition details and attach additional reference materials.
- **Delivering e-petition to the relevant state body and receiving a response.** Petitions that receive 5,000 votes will be sent to the appropriate authority. The answer with regards to the e-petition shall be provided by the authority within 30 days. The petition committee monitors meeting the deadlines and also checks if the response meets to the agreed criteria or not. The state authority should explain its answer in an easy understandable language. The official response will be published on the web platform and sent to the main applicant(s) by e-mail.

Figure 2 reflects the work process of the e-petition system designed for Azerbaijan.

6 RESEARCH LIMITATIONS AND FUTURE DIRECTIONS

This research is one of the first of its kind conducted in Azerbaijan to address the topic of e-participation and e-democracy technologies. Current study can be considered as a starting point for a number of further studies aiming to resolve democratic issues and sociopolitical problems through the introduction of the e-democracy tools like e-petition systems not only in Azerbaijan but other similar countries.

This research is a pathway for further researches in Azerbaijan addressing the topics and problems that have not been under discussion before. The authors suggests not only to focus on the

simplification and improvement of the public services provision processes but also on the involvement of the population in the public administration processes. Before actual launching of the e-petition system, a number of additional studies in this direction from different perspectives are necessary.

Moreover, the research approach of this study can be applied to investigate the practices of other developing and autocratic countries. Future research directions include comparison and analysis of different countries readiness to adopt an e-petition system.

From the limitations point of view it is likely that the results presented in this research may not cover all the e-petition systems implementation related aspects. Due to the high complexity of the e-petition system implementation process in the autocratic countries, this research can not give an exact and detailed description of all procedural related aspects. For example, issues related to the compliance framework, different deadlines and response times inside the process, required number of signatures etc. require separate studies and analysis.

Another limitations of the study is related to the survey and interview participants. It is hard to affirm that the results of the survey reflect the views and opinions of the entire population of the country. Only those citizens, who had an access to the Internet at a moment of the survey promotion, were able to take part of the survey.

It should also be noted that 78% of the respondents were aged 19-29 and the results of the survey to a greater extent reflect mostly views and opinions of this particular age group. Therefore, it is important to study other groups in more detail in the future. However, proposed e-petition model is just one additional way to enable communication with the government authorities. Therefore, current focus group is sufficient to make first steps in this field.

7 CONCLUSION

Despite the fact that e-petition systems are a relatively recent phenomenon, they are gaining popularity and are already considered an effective tool for communication and cooperation between citizens and the state, especially in developing countries. Therefore, we investigated how to design an e-petition system for developing countries similar to Azerbaijan, enabling an additional channel for citizens' participation in public decision making. The focus was to find out what benefits such a system could bring and whether the country fulfills all the necessary conditions for launching such kind of system. In that endeavour, it was also important to study the experience of different countries that launched similar systems and to identify the key factors and processes that positively resp. negatively influenced the success of these projects.

The question of what kind of barriers and difficulties might arise when an e-petition system is launched in the country, and how the population and government agencies accept it, was fundamental within this research. To answer these questions, and in order to design a model of e-petition systems for developing countries, we analyzed international experience, spread a survey among the population of Azerbaijan, and conducted four in-depth interviews with government officials. The results were positive, i.e., a large majority of citizens participating in the interviews expressed interest and willingness to take an active part if a an e-petition system would be implemented. A similar feedback was received from civil servants, who also declared their readiness and support. We also found indicators that both in technical terms and in terms of digital literacy of the population, according to the current capacity of the country, Azerbaijan would be able to launch an e-petition system.

Based on our analysis, we designed and proposed an e-petition system model for Azerbaijan that can be used also in other countries with similar background. With this study, we explored the possibility of introducing an e-petition tool in Azerbaijan and, hopefully, entail a number of other studies in this area that help in the implementation of e-participation projects in other developing countries.

ACKNOWLEDGMENTS

The work of Robert Krimmer was supported in parts by European Union's Horizon 2020 research and innovation programme under grant agreement No 857622.

REFERENCES

[1] Safura Aliyeva. 2021. Civic Engagement in Azerbaijan. *International Journal of Civil Service Reform and Practice* 5, 2 (2021).
[2] Airi-Alina Allaste and Kari Saari. 2020. Social Media and Participation in Different Socio-political Contexts: Cases of Estonia and Finland. *Young* 28, 2 (2020), 138–156.
[3] Lyudmila Bershadskaya, Andrei Chugunov, and Dmitrii Trutnev. 2013. e-Participation Development: a Comparative Study of the Russian, USA and UK e-Petition Initiatives. In *Proceedings of ICEGOV'13 – the 7th International Conference on Theory and Practice of Electronic Governance*. 73–76.
[4] Jack Blumenau. 2020. Online Activism and Dyadic Representation: Evidence from the UK e-Petition System. *Legislative Studies Quarterly* July (2020).
[5] Knud Böhle and Ulrich Riehm. 2013. e-Petition Systems and Political Participation: About Institutional Challenges and Democratic Opportunities. *First Monday* 18, 7 (2013).
[6] Lisanne de Blok, Atle Haugsgjerd, and Staffan Kumlin. 2020. Increasingly Connected? Political Distrust and Dissatisfaction with Public Services in Europe, 2008–2016. In *Welfare State Legitimacy in Times of Crisis and Austerity*. Edward Elgar Publishing.
[7] Pablo de Pedraza, Martin Guzi, and Kea Tijdens. 2020. Life Dissatisfaction and Anxiety in COVID-19 Pandemic. In *GLO Discussion Paper Series 544*. Global Labor Organization (GLO).
[8] Donna Evans and David C. Yen. 2006. E-Government: Evolving Relationship of Citizens and Government, Domestic, and International Development. *Government Information Quarterly* 23, 2 (2006), 207 – 235.
[9] Caitlin Grover. 2016. *e-Petitions*. Technical Report 1. 2204-4752. Parliament Library & Information Service, Parliament of Victoria.
[10] Loni Hagen, Teresa M Harrison, Özlem Uzuner, William May, Tim Fake, and Satya Katragadda. 2016. e-Petition Popularity: Do Linguistic and Semantic Factors Matter? *Government Information Quarterly* 33, 4 (2016), 783–795.
[11] Andreas Jungherr and Pascal Jürgens. 2010. The Political Click: Political Participation through e-Petitions in Germany. *Policy & Internet* 2, 4 (2010), 131–165.
[12] Simon Kemp. 2020. Digital 2020: Azerbaijan. (2020). https://datareportal.com/reports/digital-2020-azerbaijan.
[13] Dmytro Khutkyy. 2019. e-Participation Waves: A Reflection on the Baltic and the Eastern European Cases. *EGOV-CeDEM-ePart 2019* 197 (2019).
[14] Dmytro Khutkyy. 2019. Electronic Democracy in Belarus, Moldova, and Ukraine. Patterns and Comparative Perspectives. *Südosteuropa* 67, 2 (2019), 264–284.
[15] Ruth Kricheli, Yair Livne, and Beatriz Magaloni. 2011. Taking to the streets: Theory and evidence on protests under authoritarianism. In *APSA 2010 Annual Meeting Paper*.
[16] Onnik Krikorian, Alexey Sidorenko, and Arzu Geybullayeva. 2010. The Internet in the South Caucasus. *Caucasus Analytical Digest (CAD)* 15 (2010).
[17] Gustav Lidén. 2015. Technology and Democracy: Validity in Measurements of e-Democracy. *Democratization* 22, 4 (2015), 698–713.
[18] Ralf Lindner and Ulrich Riehm. 2011. Broadening participation through e-petitions? An empirical study of petitions to the German parliament. *Policy & Internet* 3, 1 (2011), 1–23.
[19] Giles Moss and Stephen Coleman. 2014. Deliberative manoeuvres in the digital darkness: E-Democracy policy in the UK. *The British Journal of Politics and International Relations* 16, 3 (2014), 410–427.
[20] Michael Parent, Christine A Vandebeek, and Andrew C Gemino. 2005. Building citizen trust through e-government. *Government Information Quarterly* 22, 4 (2005), 720–736.

[21] Alexander Ronzhyn. 2016. The Analysis of the Technological Platforms for E-Participation in Transition Economies of Ukraine and Russia. *Available at SSRN 3002536* (2016).
[22] Jan-Hinrik Schmidt and Katharina Johnsen. 2014. On the use of the e-petition platform of the German Bundestag. HIIG Discussion Paper Series.
[23] Barney Tan, Evelyn Ng, and Junhui Jiang. 2018. The process of Technology Leapfrogging: Case analysis of the national ICT infrastructure development journey of Azerbaijan. *International Journal of Information Management* 38, 1 (2018), 311 – 316. https://doi.org/10.1016/j.ijinfomgt.2017.10.008
[24] Maarja Toots. 2019. Why E-participation systems fail: The case of Estonia's Osale. ee. *Government Information Quarterly* 36, 3 (2019), 546–559.
[25] Robert K Yin. 2017. *Case Study Research and Applications : Design and Methods, 6xt ed.* SAGE.
[26] Seok Yoon. 2019. Azerbaijan: Country Digital Development Overview. (2019).
[27] Farhad Yusifov and Aynur Gurbanli. 2018. E-services evaluation criteria: The case of Azerbaijan. *Informacijos mokslai* 81 (2018), 18–26.

Appendix 4

IV

S. Lips, N. Bharosa, and D. Draheim. eIDAS implementation challenges: the case of Estonia and the Netherlands. In *the 7th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2020, pages 75–89, 2020

eIDAS Implementation Challenges: The Case of Estonia and the Netherlands

Silvia Lips[1(✉)], Nitesh Bharosa[2], and Dirk Draheim[1]

[1] Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia
{Silvia.lips,dirk.draheim}@taltech.ee
[2] Delft University of Technology, Postbus5, 2600 AA Delft, The Netherlands
n.bharosa@tudelft.nl

Abstract. Solid eID (electronic identification) infrastructures form the backbone of today's digital transformation. In June 2014, the European Commission adopted the eIDAS regulation (electronic identification and trust services for electronic transactions in the internal market) as a major initiative towards EU-wide eID interoperability; which receives massive attention in all EU member states in recent years. As a joint effort of Estonia and the Netherlands, this study provides a comparative case study on eIDAS implementation practices of the two countries. The aim was to analyze eIDAS implementation challenges of the two countries and to propose a variety of possible solutions to overcome them. During an action learning workshop in November 2019, key experts from Estonia and the Netherlands identified eIDAS implementation challenges and proposed possible solutions to the problems from the policy maker, the service provider and the user perspective. As a result, we identified five themes of common challenges: compliance issues, interpretation problems, different practices in member states, cooperation and collaboration barriers, and representation of legal persons. Proposed solutions do not only involve changes in the eIDAS regulation, but different actions to develop an eIDAS framework and to improve cross-border service provision - which has recently become an important topic among member states. Eventually, the study provides practical input to the ongoing eIDAS review process and can help member states to overcome eIDAS implementation challenges.

AQ1

Keywords: eIDAS · Electronic authentication · Electronic identity · Implementation challenges · Identity management

1 Introduction

Digital transformation of countries offers many opportunities, but at the same time reduces control over their operating environment [1]. More and more, public and private sector organisations offer their services online and across borders. To access these e-services, implementation of an accurate and reliable digital authentication procedure together with a digital signature option is essential [2, 3].

A. Chugunov et al. (Eds.): EGOSE 2020, CCIS 1349, pp. 1–15, 2020.
https://doi.org/10.1007/978-3-030-67238-6_6

In July 2014, the European Commission (EC) adopted regulation No 910/2014 [4] on electronic identification and trust services for electronic transactions in the internal market (eIDAS) to enable a secure and seamless electronic data exchange and interaction of public and private entities and users, not only inside the member states, but also across the European Union (EU). This initiative is part of the EU Digital Single Market strategy [5] and mandatory for all EU member states since September 2018 [4].

The implementation of the eIDAS regulation and its first years of implementation have raised many practical questions and revealed various research gaps. According to the eIDAS regulation Article 49, the EC shall review the regulation by 01.07.2020 latest to evaluate whether the regulation needs to be modified [4]. The EC has already initiated a feedback collection process among its member states. In parallel with the ongoing eIDAS implementation actions, EC progressed further and adopted in October 2018 SDGR regulation, which established a single digital gateway to provide access to information, procedures and for assistance and problem-solving services, also known as the SDGR regulation [6]. The aim of this regulation is to simplify access to cross-border administrative services for citizens and companies [7]. One pre-condition for the SDGR implementation is successful and smooth eIDAS implementation in the member states. Therefore, it is now the perfect time to analyze the implementation practices of different EU countries and to provide relevant feedback to the ongoing evaluation process.

We decided to research the practices of Estonia and the Netherlands. Both of the countries have stable and functional e-government, but at the same time, they have different e-governance models and approaches to the eIDAS implementation [8].

The aim of this research paper is to analyze eIDAS implementation challenges of Estonia and the Netherlands and to propose a variety of possible solutions to overcome them. The research objectives are therefore to:

1) Identify the challenges Estonia and the Netherlands faced during the implementation of eIDAS from the user's, the service provider's and the policy maker's perspective; and
2) Recommend possible solutions to overcoming identified challenges.

We use a comparative case study research approach [9] together with action learning methodology [10] to analyse above-mentioned research questions.

The paper is organized as follows. Section 2 provides background information about the current eIDAS implementation situation in Estonia and the Netherlands and an overview of important related literature. Section 3 presents the research design and gives insight into the used theoretical framework. Section 4 sums up research findings from the policy maker, service provider and user perspective. In Sect. 5, we discuss the research results and make recommendations to the eIDAS review process. Section 6 provides an insight to the future research perspective followed by Sect. 7 that concludes the study.

2 Background

In this section, we provide a brief overview of existing literature on eIDAS implementation. In addition, to understand the results of this paper, it is important to introduce shortly the eIDAS implementation state and situation in Estonia and the Netherlands.

2.1 eIDAS Implementation in the EU from the Literature Perspective

The eIDAS regulation has been in force for more than five years, of which it has been actively implemented and used over the past two years. According to the regulation itself, voluntary recognition of electronic identities were possible since September 2015, rules for trust service providers had to be adopted by July 2016 and cross-border recognition of electronic identities was enabled by September 2018 [5]. First countries notified their eID schemes[1] under eIDAS already in 2017 (Germany) and 2018 (Estonia, Spain, Croatia, Belgium etc.). The implementation process itself is complex and time-consuming. Figure 1 illustrates the steps that member states have to pass to notify their eID schemes.

Fig. 1. eID scheme notification process.

From a research perspective, the topic is quite new; and, so far, it has been handled rather from the angle of a specific country or sector. For example, several studies focus on the academic sector, e.g., on how to build eIDAS-based cross-border services in the education and to enable secure and seamless interaction between different parties [11–15]. The focus is mainly on solving the practical problems: how to transport new data attributes through eIDAS infrastructure solutions [11, 13], how to implement eIDAS-based academic services and create secure connections between academic services and the national eIDAS node [12, 13]. Some studies are even more specific and concentrate on a part of an eIDAS node that member states have to modify independently [14].

Several studies focus on eIDAS implementation challenges in a particular country [16–18]. In case of United Kingdom (UK), it is questionable if the country should notify their eID scheme and does the existing system complies with the eIDAS privacy and data protection requirements [17]. Pelikánová, Cvik and MacGregor analyze and

[1] According to eIDAS, an eID scheme is a system for electronic identification under which electronic identification means are issued to natural or legal persons (or to natural persons representing legal persons).

evaluate the eIDAS adoption in the Czech public sector bodies and compare the results with some other EU member states practice. Their research results show a lot of hesitation and passivity in the Czech public sector while adopting eIDAS requirements [18].

Other research projects focus more on different aspects of the regulation, such as security, privacy [19, 20] and data protection issues [21]. From the data protection perspective, Tsakalakis, Stalla-Bourdillon and O'Hara argue that technical architecture of an eID scheme affects the level of data protection. They propose that the use of pseudonyms and selective disclosure help to fulfill the data minimization and purpose limitation principles [21]. Only few studies analyze different identification and trust services compatible with the eIDAS regulation in wider context and do not focus on a particular member state [22].

While conducting the literature overview it became clear that many of the studies focus on specific sectors or solve very concrete data exchange or integration issues in the eIDAS context. We did not find pan-European studies addressing eIDAS implementation practices in various member states with proposals to improve the current environment. Therefore, our research aims to fill this significant research gap and to provide recommendations for the further eIDAS review process.

2.2 Estonia

Estonia has implemented eIDAS according to the EC timetable and notified its eID scheme on assurance level "high" in November 2018. The notification consisted of six different eID tokens: ID-card, residence permit card, digital identity card, e-residency digital identity card, mobile-ID and diplomatic identity card.[2]

The Estonian eID management is based on tight public-private cooperation. Public sector authorities are responsible for personal identification, identity management, eID infrastructure management and supervisory activities. Private sector organization offers eID tokens as well as personalization and trust services [23]. In December 2018, Estonia changed the eID token manufacturer and since then, has issued the fourth generation electronic of identity cards [24].

All previously mentioned electronic identities are in active use and the public acceptance of the eID is high [25, 26]. According to the latest statistics from March 2020, there are more than 1,35 million eID cards and around 234 000 mobile-ID´s issued by the public sector. In February 2020, the total amount of transactions related to eID´s exceeded 37 million.[3]

[2] Estonian eID scheme notified under eIDAS, https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia.

[3] Estonian eID statistics, https://www.id.ee/?lang=en&id=.

In addition to the public sector eID tokens, the local trust service provider SK ID Solutions AS issues QSCD (Qualified Signature Creation Device) certified Smart-ID for authentication and signing purposes.[4] More than 500 000 users also actively use this solution.[5]

2.3 The Netherlands

In 2019, the Netherlands notified its electronic identification trust framework for businesses, also known as eHerkenning, on the assurance levels "substantial" and "high".[6] There are several authentication service providers in the country (i.e., Connectis, Digidentity, KPN, QuoVadis, Reconi, and Unified Post).[7]

In December 2019, the Netherlands pre-notified another authentication service named "DigiD. This solution enables authentication of natural persons in relation with the governmental authorities and organizations that perform public tasks. Logius, an organization operating in the governing area of the Dutch Ministry of the Interior and Kingdom Relations, manages and maintains the DigiD in the Netherlands [27].

Around 80% (14 million people) of the Dutch population use the service. More than 650 service providers are connected to the DigiD service. According to the statistics, DigiD service processes over 300 million authentication requests per year.[8]

The Netherlands is currently working towards the next generation DigiD solution called "DigiD hoog". The solution will be more secure and will base on the Dutch identity card and driving license information [27]. The Netherlands also tries to integrate biometrical features into their national authentication scheme.

3 Research Design

In this research, we conduct a comparative case study on eIDAS implementation in the Netherlands and Estonia. For this purpose, we gathered an expert team and used action learning [10, 28] to compare the eIDAS implementation challenges of Estonia and the Netherlands and to find possible solutions to identified problems. Action learning [10, 28] is particularly well suited to research complex phenomena such as eIDAS [29].

One of the alternative research designs was a world café approach [30], but as the focus of this particular method is more on generating broader range of perspectives than to find answers, we found action learning more appropriate for, this study.

[4] Smart-ID's recognition as Qualified Signature Creation Device (QSCD), https://www.smart-id.com/e-service-providers/smart-id-as-a-qscd/.

[5] Estonian eID statistics, https://www.id.ee/?lang=en&id=.

[6] The Netherlands (DTF/eHerkenning) eID scheme notified under eIDAS, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=74091935.

[7] Dutch Trust framework for Electronic Identification, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=74091935.

[8] The Netherlands (DigiD) scheme pre-notified under eIDAS, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=176620999.

The research relies on an international collaboration between researchers, public and private sector experts from the Netherlands and Estonia. The Netherland authority Digicampus[9] coordinated and facilitated the cooperation. The Digicampus is an innovation hub that connects science, government, market players and citizens/users to shape future public services. Figure 2 illustrates action-learning-based collaboration between the Netherlands and Estonia [28].

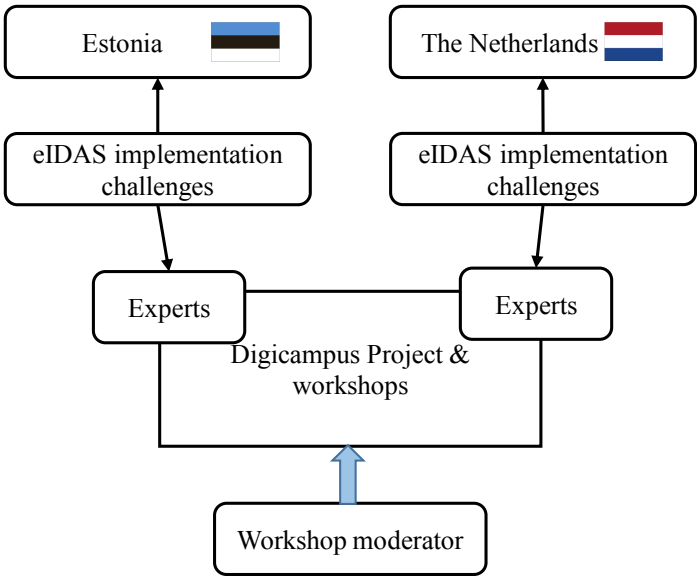

Fig. 2. Project structure and participants.

As a result of the cooperation, two expert workshop sessions on (i) eIDAS implementation challenges and (ii) in service of finding possible solutions have been held at Tallinn University of Technology, Estonia, from November 18 to 21, 2019. Nine experts from Estonia and 14 experts from the Netherlands have been involved. Table 1 provides a detailed overview of the participants and their roles.

During the workshop sessions, we divided all participants into three groups presenting policy makers, the private sector and users. All groups consisted of participants from both countries. The first workshop took place on 19.11.2020, where experts shared their practical experience and challenges with the eIDAS implementation.

On the next day, the same groups continued working together and tried to find solutions to these challenges. After group work on both days, each group presented its result and the other groups had an opportunity to supplement it.

[9] Digicampus homepage, https://www.dedigicampus.nl/.

Table 1. Project structure and participants.

Estonia		The Netherlands	
Organization	Role	Organization	Role
Information System Authority	Head of eID department	Ministry of the Interior and Kingdom Relations	Policy officer (digital government)
	Product owner (eIDAS cross-border usage)		Senior advisor (member of the Dutch eIDAS team)
Police and Border Guard Board	Adviser-expert (eIDAS implementation, auditing)		eHerkenning project manager
	Chief-expert (eIDAS SPOC)		Strategic advisor
Ministry of Economic Affairs and Communications	Adviser (SDG national coordination)	Municipality of Den Haag	Advisor (digital transformation)
SK ID Solutions AS	Lawyer (trust services, eIDAS, ETSI EN standards, national law)		Product owner (digitalization and authentication)
TalTech	Full Professor of Information Systems (e-governance and technologies)	TU Delft	Senior researcher Master students (2)
		Agentschap Telecom	Supervision of eIDs
		ICTU	Sr advisor Program manager
	Researcher (eIDAS framework)	Netherlands Enterprise Agency	Product owner (International Access)
	Researcher (public acceptance of eID)	Private sector representatives	Four persons

4 Findings

In this section, we present our research findings from three different perspectives: policy maker, service provider and user perspective. We focus mainly on the eIDAS implementation problematics and do not reflect the discussions regarding other relevant topics more or less related to eIDAS, like applicability of the once-only principle (OOP) [31] or the implementation of the SDGR regulation.

4.1 Challenges and Solutions from the Policy Maker Perspective

From the policy maker perspective, we identified challenges related to the following issues: *implementation, (national) legislation, interpretation, compliance and communication.*

A crucial eIDAS implementation barrier is the lack of the EU common identifier. It is still not possible to use national eIDs and digital signatures for EU services. Particularly problematic is when users would like to act on behalf of others despite of sufficient legal grounds. The experts found that it is important to find a workaround or initiate further discussions on the EU common identifier to overcome this barrier. These challenges concern both natural and legal persons; and the topic should be added to the further research agenda.

The experts found that slight differences in the national laws complicate the uniform eIDAS implementation process in the EU. For example, according to the national laws, the actions that minors are allowed to perform varies from country to country. This affects, in particular, the establishment of cross-border services.

From the legal person's perspective, eIDAS allows for company eIDs without persons attached to it. This raises several practical questions. For instance, how to make it possible that a person is allowed to act on behalf of a company? How to use a legal person eID across borders? It is important to define all the issues related to legal persons separately and provide feedback to the eIDAS review process.

Representatives of the policy maker group considered interpretation of the eIDAS regulation as a crucial challenge. For example, Article 6 (that regulates mutual recognition of eIDs) is ambiguous. In addition, it is not clear how to map existing technologies to eIDAS assurance levels and how to assess their risks.

The experts identified the following shortcomings at the level of compliancy:

- not all member states offer eID;
- lack of supervision;
- the EC executes its supervisory role only weakly;
- the member states do not always accept each other's eIDs (e.g. Germany/Estonia);
- it lacks a framework for conformity assessment on the EU-level;
- There are no common rules for supervisory bodies.

The creation of assessment guidelines for auditors would help significantly to overcome the previously identified issues. Another solution that experts considered was the integration of ethical hacking into the eIDAS framework in order to improve existing requirements.

Finally, the experts agreed that the current SDG (Single Digital Gateway) program should have a stronger link to the eIDAS regulation and implementation activities. They also noted, that communication activities (i.e., why it is important to implement eIDAS) from the EU side should be improved.

4.2 Challenges and Solutions from the Service Provider Perspective

From the service provider perspective, we identified challenges related to the following issues: *collaboration, compliancy, reputation, change management, notification and record matching*.

The experts found a crucial challenge that lies on a co-operational level. It is not clear how to combine different competences in case of incidents (problem ownership issue). Applying EU wide user testing and meta-research on the cross-border collaboration level would help to solve this issue.

There exist no common rules for service providers on how to comply with the eIDAS regulation. Service providers are unsure, how to test their systems, i.e. how to understand whether their systems are compliant or not. Therefore, a standardized test framework with test data would be very helpful (e.g., a standard backward-compatible API).

Different change management issues complicate the eIDAS implementation process. It is not easy to keep up with changing standards and regulations. Often, changes are unpredictable and require remarkable additional investments. Misinterpretation of requirements can cause unnecessary additional work and costs. The experts found that eIDAS could be provided as a service for all public and private authorities (e.g. "spin a node and go"). Exploiting the World Wide Web Consortium (W3C), decentralized identifier (DiD) as a unique identifier (UiD) seems promising, but needs further in-depth research.

The eIDAS regulation provides no guidelines and standards for unique identifiers of persons (i.e., mandatory vs. free attributes, registration of foreign identities, tracking etc.). There is also lack of a common architecture API platform. The experts found that use of decentralized identifiers and identity linking would help to overcome the previously identified issues.

Notification of private sector solutions is a complex topic. Private sector service providers has no access to the data in the scope of the eIDAS regulation. However, fully automated and cross-border services need person related data. In this case, a common understanding of trust and privacy models plays an important role.

The experts found, that reputation is also an important topic, dependent on the reputation of all participants acting inside the eIDAS framework. The eIDAS framework is based on trust, but the meaning of *trust* differs in different cultures.

4.3 Challenges and Solutions from User Perspective

The user perspective covers a variety of challenges starting from usability to security and privacy concerns.

Accessibility and user experience (UX) of cross-border services needs improvement through additional guidelines, templates, examples, UX tests, experience and sharing of best practices. The same service may have a completely different user experience in different countries. This makes it difficult to find the right services abroad. In this case, standardized service portals that direct people to the right place, would be helpful. The experts also discussed language support and semantics problems that can be overcome by organizing learning courses and by describing step-by-step use cases.

From the security perspective, users have to understand whether they are using qualified services to avoid possible "man in the middle" attacks. Security awareness can be increased by developing guidelines, templates, sharing best practices and educating users continuously.

There is also a need for a governance framework and clear role division, as users often do not know whom to contact in case of technical error, usability problems or other relevant questions.

The experts discussed how to avoid errors and how to deal with service continuity when certificates become invalid. A would help solving this issue.

Finally, the experts found the current cross-border roles and mandates are insufficient. For example, users are unable to act on behalf of a legal person that they represent. From that perspective, the experts suggested that the scope of eIDAS regulation should contain the procedures related to the legal persons. They also proposed introduction of an EU common identifier.

5 Discussion and Recommendations

Based on our research results, it is clear that eIDAS implementation process is challenging from various perspectives. Policy makers, service providers and users have different expectations and needs. Based on the workshop results, where experts offered solutions to the eIDAS implementation challenges, we identified five main themes that all groups mentioned during the workshops in one or another way. These five common challenges are:

- compliance issues;
- interpretation problems;
- different practices in member states;
- co-operation and collaboration barriers;
- legal persons and their representation.

Compliance issues include insufficient guidelines (and supervision) for public service providers, private sector service providers and conformity assessment bodies. In this situation, parties start to interpret the requirements according to their practice; and this leads to the problem of different interpretations, starting from the usage of terminology to system usability issues. All identified challenges create additional communication and collaboration barriers between service providers and users as well as between EU member states.

Another interesting finding from the workshops is that most of the challenges are related with cross-border service provision rather than eIDAS implementation inside countries. Existing rules and requirements support the implementation of eIDAS inside member states, but are not sufficient to support the EU-wide implementation.

Table 2 provides detailed summary of eIDAS implementation related challenges and solutions from all three perspectives.

During the workshop, the experts discussed various options to overcome existing challenges and improve the eIDAS implementation process. Therefore, European Commission could consider the following proposals in the upcoming eIDAS review process:

- options to implement a common EU identifier;
- regulate the identification of users so that they can act on behalf of others when legally required;
- specify the regulation with respect to legal persons;
- clarify the terminology of the eIDAS regulation;

Table 2. Summary of eIDAS related challenges and solutions.

	Category	Challenges	Solutions
Policy maker	Implementation	No EU wide identifier	Workaround
		Acting on behalf of others	Workaround
		National eIDs/digital signatures are not usable for EU services	Initiating further discussions on the EU common identifier
	Legislation	Different legal practices in Member States	Creation of assessment guidelines for auditors
	Interpretation	Differences in the interpretation of the eIDAS articles	Creation of assessment guidelines for auditors
	Compliance	Different shortcomings	Creation of assessment guidelines for auditors
	Communication	eIDAS implementation importance	Communication plan
Service provider	Collaboration	Problem ownership issue	EU wide user testing
			Meta-research on the cross-border collaboration
	Compliancy	Compliancy of service providers	Standardized test framework with test data
	Change management	Changing regulations, standards	eIDAS provided as a service
	Notification	Notification of private sector solutions	Common understanding of trust and privacy models
	Record matching	No standards for unique identifiers/lack of common architecture	Common architecture API platform
			Use of decentralized identifiers
			Identity linking
User	Usability	UI consistence usage	Additional guidelines, templates, examples, UX testing, experience and sharing of best practices
		Accessibility to e-services	
		Different countries have different practices	Standardized service portals
	Helpdesk/ Support	User support in case of errors	Clear role division
		Language support and semantics	Courses, step-by-step use cases
	Security	Possible “Man in the middle” issue	Guidelines, templates, sharing best practices, user education
		“Dirty error” issue when certificates are invalid	Central monitoring service

- clarify often misinterpreted articles in the eIDAS regulation;
- develop common assessment guidelines for auditors;
- develop a standardized testing framework;
- provide eIDAS as a service;
- create a common monitoring system for cross-border transactions;
- develop a framework of standards for cross-border services.

Not all of these proposals and activities presume changes in the eIDAS regulation. Many of these initiatives require further discussion between the member states and more detailed analysis by the responsible organizations.

6 Future Directions

Current research is a part of a larger research project regarding the eIDAS, which aims to improve its compliancy assessment model. To develop this model we analyze and compare the eID schemes of different member states and their eIDAS implementation practice.

During this particular research, we identified various topics and questions that need further in-depth research and analysis. For example: requirements and preconditions for the application of a common EU identifier; creation of assessment guidelines for auditors, implementation of EU wide user-testing environment; cross-border service provision; collaboration between public service providers and private sector service providers. These topics will address in the scope of further research actions.

We hope that the outcome of the whole study is a valuable tool for the public and private sector eID service providers and auditors enabling more transparent and comparable assessment of different eID schemes. Moreover, our research results will be the basis for the further universal applicability analysis of the eIDAS principles while implementing SDGR regulation and establishing secure e-service provision between EU and third countries.

7 Conclusion and Research Limitations

This study showed that different EU member states have faced similar problems in the eIDAS implementation process and that it is important to exchange practical experiences at the expert level.

From the limitations point of view, it is not possible to compile a complete list of challenges based on the experience of just two countries. Additionally, offered solutions and recommendations reflect the knowledge and experience of the experts who participated in the workshops. It means that there can be other alternative ways to overcome the identified challenges. However, we are convinced that the results indicate to major shortcomings and practical problems that member states face during an eIDAS implementation.

Based on our research results, it is possible to say that the focus of the member states (with respect to the implementation of eIDAS and in light of the SDGR regulation) has clearly shifted from a national level to a cross-border perspective. However, before taking this next step in terms of cross-border service integration it is important to ensure stable and interoperable network of eIDs.

We identified five challenging areas (compliance issues, interpretation problems, different practices in member states, co-operation and collaboration barriers, legal persons and their representation) in the eIDAS implementation process, which will inevitably affect the implementation of other related regulations.

This new situation requires a review of the existing EU eIDAS framework and procedures by the European Commission. Our study provides practical input to the eIDAS review process by identifying common challenges of the member states and making proposals to overcome them.

References

1. Vial, G.: Understanding digital transformation: a review and a research agenda. J. Strateg. Inf. Syst. **28**(2), 118–144 (2019)
2. 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
3. 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
4. European Parliament and Council: EU Parliament and Council regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC (2014)
5. The European Parliament: EU Parliament Resolution. Towards a Digital Single Market Act (2015/2147(INI) (2016)
6. European Parliament and Council: EU Parliament and Council Regulation (EU) No 2018/1724 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (2018)
7. Bhattarai, R., Pappel, I., Vainsalu, H., Yahia, S.B., Draheim, D.: The impact of the single digital gateway regulation from the citizens' perspective. Procedia Comput. Sci. **164**, 159–167 (2019)
8. Bharosa, N., Lips, S., Draheim, D.: Making e-government work: learning from the Netherlands and Estonia. In: Hofmann, S., Csáki, C., Edelmann, N., Lampoltshammer, T., Melin, U., Parycek, P., Schwabe, G., Tambouris, E. (eds.) ePart 2020. LNCS, vol. 12220, pp. 41–53. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58141-1_4
9. Yin, R.K.: Applications of Case Study Research. Sage, Thousand Oaks (2011)
10. Revans, R.W.: ABC of Action Learning. Gower Publishing, Ltd., Farnham (2011)
11. Berbecaru, D., Lioy, A., Cameroni, C.: Electronic identification for universities: building cross-border services based on the eIDAS infrastructure. Information **10**(6), 210 (2019)

12. Maliappis, M., Gerakos, K., Costopoulou, C., Ntaliani, M.: Authenticated academic services through eIDAS. Int. J. Electron. Gov. **11**(3/4), 386 (2019)
13. Klobučar, T.: Improving cross-border educational services with eIDAS. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S. (eds.) WorldCIST'19 2019. AISC, vol. 931, pp. 932–938. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16184-2_88
14. Berbecaru, D., Lioy, A., Cameroni, C.: Providing digital identity and academic attributes through European eID infrastructures: results achieved, limitations, and future steps. Softw. Pract. Exp. **49**(11), 1643–1662 (2019)
15. Gerakos, K., Maliappis, M., Costopoulou, C., Ntaliani, M.: Electronic authentication for university transactions using eIDAS. In: Katsikas, S.K., Zorkadis, V. (eds.) e-Democracy 2017. CCIS, vol. 792, pp. 187–195. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-71117-1_13
16. Vogt, T.: Die neue eIDAS-verordnung – chance und herausforderung für die öffentliche verwaltung in deutschland. Inf. Wissenschaft Praxis **67**(1), 61–68 (2016)
17. Tsakalakis, N., OHara, K., Stalla-Bourdillon, S.: Identity assurance in the UK. In: Proceedings of WebSci 16 - The 8th ACM Conference on Web Science. ACM Press (2016)
18. Pelikánová, R.M., Cvik, E.D., MacGregor, R.: Qualified electronic signature – eIDAS striking czech public sector bodies. Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis **67**(6), 1551–1560 (2019)
19. Engelbertz, N., Erinola, N., Herring, D., Somorovsky, J., Mladenov, V., Schwenk, J.: Security analysis of eidas – the cross-country authentication scheme in europe. In: 12th USENIX Workshop on Offensive Technologies (WOOT 2018). USENIX Association, Baltimore, MD, August 2018
20. Kutyłowski, M., Hanzlik, L., Kluczniak, K.: Pseudonymous signature on eIDAS token – implementation based privacy threats. In: Liu, J.K., Steinfeld, R. (eds.) ACISP 2016. LNCS, vol. 9723, pp. 467–477. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_31
21. Tsakalakis, N., Stalla-Bourdillon, S., O'Hara, K.: Data protection by design for cross-border electronic identification: does the eIDAS interoperability framework need to be modernised? In: Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S. (eds.) Privacy and Identity 2018. IAICT, vol. 547, pp. 255–274. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16744-8_17
22. Mocanu, S., Chiriac, A.M., Popa, C., Dobrescu, R., Saru, D.: Identification and trust techniques compatible with eIDAS regulation. In: Li, J., Liu, Z., Peng, H. (eds.) SPNCE 2019. LNICST, vol. 284, pp. 656–665. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21373-2_55
23. 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
24. 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
25. 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

26. 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
27. Roelofs, F.: Analysis and comparison of identification and authentication systems under the eIDAS regulation. Master's thesis, Radboud University, the Netherlands (2019)
28. Pedler, M.: Action Learning in Practice. Gower Publishing, Farnham (2011)
29. Zuber-Skerritt, O.: Action learning and action research: paradigm, praxis and programs. In: Effective Change Management Through Action Research and Action Learning: Concepts, Perspectives, Processes and Applications, vol. 1, p. 20 (2001)
30. Aldred, R.: From community participation to organizational therapy? World cafe and appreciative inquiry as research methods. Commun. Dev. J. **46**, 57–71 (2009)
31. Wimmer, M.A., Tambouris, E., Krimmer, R., Gil-Garcia, J.R., Chatfield, A.T.: Once only principle. In: Proceedings of the 18th Annual International Conference on Digital Government Research. ACM (2017)

Appendix 5

V

S. Lips, K. Aas, I. Pappel, and D. Draheim. Designing an effective long-term identity management strategy for a mature e-state. In *the 8th Electronic Government and the Information Systems Perspective*, EGOVIS 2019, pages 221–234, Cham, 2019. Springer

Designing an Effective Long-Term Identity Management Strategy for a Mature e-State

Silvia Lips[1(✉)], Krista Aas[2], Ingrid Pappel[1], and Dirk Draheim[1]

[1] Tallinn University of Technology, Akadeemia tee 15a, Tallinn 12616, Estonia
{silvia.lips,ingrid.pappel,dirk.draheim}@taltech.ee
[2] Estonian Police and Border Guard Board, Pärnu mnt 139, Tallinn 15060, Estonia
krista.aas@politsei.ee

Abstract. Countries that have a well-functioning e-governance ecosystem (infrastructure, processes, interoperability network, user-friendly e-services etc.) reach a particularly high e-governance maturity level. To ensure continuous development and adoption to the changing technological environment the systematic consideration of users' needs is important in the definition of long-term strategical goals. Identity management is a corner stone of each mature e-governance ecosystem. This paper focuses on the process of creating the new Estonian strategy for identity management and identity documents and the analysis of this process from different aspects (responsibilities, engaged stakeholders and interest groups, key competences, scope, implementation). In addition, we give an overview of the underlying strategical and legal regulatory framework. The objective is to map the best practices and bottlenecks of the strategy creation process and propose a model for area specific long-term strategical documents. We aim at understanding best practices and bottlenecks in the process of creating the ID strategy. In service of this, we have conducted qualitative interviews with several high-ranking experts that have been involved as stakeholders in the strategy building process. Based on this, we propose a model for area-specific long-term strategical documents. Furthermore, the research results indicate that it is necessary to invest continuously into public-private partnership.

Keywords: Identity management · Strategy building · Electronic identity · Change management

1 Introduction

Estonia has significant experience in the field of e-governance and e-services from almost twenty years. The established PKI (public key infrastructure)-based e-governance system is intensively used. 98% of the Estonian population have an ID-card that hosts an eID (electronic identity) token; and about 2/3 of them use it regularly. During these twenty years, more than 500 million digital signatures has been given and, at the present time, it is possible to use more than 5000 e-services [1].

Since 2002, the system has remained quite similar with only minor changes. In the end of the year 2018, new contract partner started to issue the fourth generation of eID

A. Kő et al. (Eds.): EGOVIS 2019, LNCS 11709, pp. 221–234, 2019.
https://doi.org/10.1007/978-3-030-27523-5_16

documents. It is clear that the whole system has reached to the maturity level where dealing with concrete developments or needs is not sufficient and there is a clear need for an overall framework and long-term development strategy. Therefore, in September 2017, the Estonian Police and Border Guard Board (PBGB) together with the Estonian Information System Authority (EISA) initiated a process at the level of the public and the private sector level to agree on a long-term identity management view. The process lasted almost one and a half years and resulted into a white paper on identity management and identity documents, henceforth abbreviated as IMIDS white paper or just IMIDS for short.

The current article concentrates mainly on the creation process of the IMIDS white paper and not so much on analyzing the content of the document. The aim is to map the best practices and design an effective model for mature e-states who feel the need for a long-term view.

During the process, common understanding on the terminology level is crucial. If we talk about identity management and identity documents, then it is important to understand the meaning of the term "identity management". There is no single definition of identity management. On a very general level identity management is a security system, which authorizes users to access to certain information or systems [2]. In the current context, identity management means keeping consistent record of a person's identity and managing it by the state during its whole lifecycle. Identity documents are all documents issued by the state and stated in the Identity Documents Act paragraph 2 Section 2 [3]. It means identity card and digital identity card (including e-residency digital identity card), residence permit card, diplomatic identity card, 7 types of travel documents (passports) and mobile-ID [4].

Taking into account previously described framework, it is important to emphasize that in this article we do not focus only on the electronic part of the identity management because the strategical view is much broader covering additionally physical identity management issues, tokens, physical identity carriers, data protection, security issues etc.

In addition, if we talk about identity management and identity documents strategical view then at the same time, we talk at least partly about the strategic management of related information systems and IT innovation. Therefore, it is important to understand if there is an actual need and will for innovation and this type of long-term strategy. The same question raised during the IMIDS creation process – does Estonia actually want to be an innovative and leading country in terms of identity management and eID. According to the answers, Estonia clearly wants to be a successful e-country, but this also means that the country shall be ready for early adoption of new technologies and/or applications [5]. From that point of view, it is crucial to have a long-term perspective and common understating in the identity management area ensuring the implementation and funding of the innovative ideas, solutions and increase user satisfaction [6].

This article contains three main chapters. Firstly, we formulate the research problem and give methodological background with related frameworks. Then, we give an overview about the identity management and identity documents strategy building process and outcomes and analyze different aspects of the process. Finally, we present the most important and interesting findings.

2 Problem Formulation and Frameworks

2.1 Problem Formulation and Theoretical Framework

Central question of the current article is about designing an effective long-term identity management and identity documents strategy for a mature e-state through public and private cooperation. We analyze different aspects like responsibilities, engaged stakeholders and interest groups, key competences, scope and implementation issues. To support the main theme, we give an overview about the identity management and identity documents creation process, outcomes and propose a model of best practices.

Our research methodology is oriented towards action design research (ADR) as we were involved directly to the IMIDS creation process [7]. After the strategy document was ready, we conducted twelve individual structured non-standardized interviews with public and private sector experts who participated in the process (approximate duration one hour each). Five interviewees from the twelve were public and seven private sector representatives. Some of the examples of interviewees: PBGB head of identity and status bureau, EISA head of eID branch, CEO of SK ID Solutions AS, head of citizen markets of IDEMIA, CEO and vice-president of the Estonian Association of Information Technology and Telecommunications (ITL) etc.

Theoretical background of this article bases on the three main concepts: identity theory [8], change management [9] and public private partnership (PPP) [10]. All previously named concepts relate and supplement each other.

2.2 Strategical and Regulatory Framework

In the context of building the national identity management strategy, it is important to understand what kind of legal and strategical documents already exist and how they influence the area. Political and vision documents that has no direct legal impact and legislative acts having direct juridical impact must be distinguished.

On the state level there are in total 47 strategical documents. They are all different in terms of their juridical status, structure, purpose and their relation to the state budget [11]. Directly connected to the identity management area are only two of them: Internal Security Development Plan (STAK) and Estonian Information Society Development Plan (EISDP).

Internal Security Development Plan has eight sub programs and one of the programs is reliable and secure identity management that contains following three main policy instruments: development of secure and smart solutions, effective and systematic administration and management of the identity area, ensuring high quality personal data [12].

EISDP is more detailed policy document focusing inter alia to the eID area. The main aim of the document is to find smart solutions how to use ICT and solve nationwide challenges [13].

Juridical framework is more determined and has direct binding effect to the parties. Therefore, it is important to have an overview of the existing legal regulations related to the identity management and identity documents area. In addition to that, it is important to remark that new technological approaches and innovative solutions might presume

changes in the existing legal environment or even establishing new regulatory framework.

Legal framework in the identity management and identity documents area has conditionally three main layers: pre-juridical framework, international law and EU legislation and state law (Fig. 1).

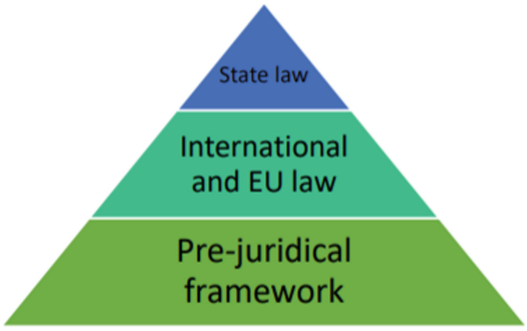

Fig. 1. Identity management legal framework layers.

Pre-juridical framework plays an important role especially in the identity management field consisting different technical standards (ISO, ETSI, PCI etc.) and recommendations (ICAO 9303 etc.) [14]. Even these documents do not have direct juridical impact, they are recognized and accepted worldwide and often used, referenced similarly to legal acts. International and EU law level is a set of different directives and directly applicable regulations that directly or indirectly relate to the identity management area.

On the state level, the main legal acts regulating the identity management regulatory environment in Estonia are Identity Documents Act and Electronic Identification and Trust Services for Electronic Transactions Act [4, 15].

3 Identity Management Strategy Building Process and Outcome

3.1 Strategy Building Process

Estonian identity management field (including eID ecosystem) is complex environment engaging public and private sector expertise and based on a close cooperation of both sectors. It is a well-operating network consisting of different players and roles [16].

During the first half of 2017, EISA initiated to PBGB that they would like to have a long-term view on the eID field. As the topic is wider than digital identity and eID,

parties started to build the identity management strategy. 22.09.2017 PBGB and EISA sent an official IMIDS creation proposal to the public sector stakeholders.[1]

Based on the initiative 04.10.2017 public sector stakeholders met in the PBGB. Representatives of three different ministries (Ministry of the Interior, Ministry of Foreign Affairs and Ministry of Economic Affairs and Communications) participated. One of the main concerns brought out in the meeting was the juridical status of the planned strategical document. PBGB and EISA explained that the document becomes an input for already existing political strategical documents. It was clear that public sector did not have a common understanding of different identity management related issues. Therefore, the representatives decided that firstly it is important to achieve common understanding among public sector authorities and then engage private sector stakeholders.

First workshop for public sector stakeholders was 01.12.2017. After brief introduction, the work continued in two main sections: (1) electronic identity and related services (2) physical identity management and related topics. During the first part of the workshop on both sections' participants listed all bottlenecks and shortcomings related to the theme. After that, solution brainstorming followed. The aim was to find innovative solutions to the existing problems and try to think without borders. Finally, both groups presented their results and findings.

Based on the 01.12.2017 workshop results PBGB decided to have one additional internal workshop on 16.01.2018 where all service owners in the PBGB identity and status bureau and one representative of EISA participated. The aim was to think through together once more the broader picture and create links and synergies between different services. Based on the results of these two workshops first draft of the IMIDS was created and sent 02.02.2018 to the PBGB and EISA and shortly after to other public sector stakeholders.

The first draft based on the overlapping part of the mission and vision of the PBGB and EISA, as they are main implementing authorities on the identity management and identity documents field. Second workshop for public sector stakeholders was 03.04.2018. The focus of the meeting was to discuss the received feedback and make amendments to the IMIDS documentation.

01.06.2018 PBGB sent the IMIDS draft to the private sector stakeholders together with a meeting proposal.[2] The meeting was at EISA on 19.06.2018. EISA and PBGB introduced the IMIDS documentation and principles, open discussion followed. Private sector was clearly cautious and expressed their disappointment not being on engaged to the process already earlier. It was clear that there is a need for more meetings.

IMIDS documentation was little bit modified and 06.09.2018 next meeting was held. During the meeting, experts decided to change the document structure. Therefore, the decision was that before planned workshop in October 2018 public and private

[1] Ministry of the Interior, Ministry of Economic Affairs and Communication, IT and development center (SMIT), Tallinn Technical University (TeleTech), Estonian Data Protection Inspectorate, former Technical Regulatory Authority now known as Consumer Protection and Technical Regulatory Authority and Centre of Registers and Information Systems.

[2] SK ID Solutions AS, ITL, Estonian Banking Association, Cybernetica AS, Guardtime AS and IDEMIA - representing the interest of information technology companies.

sector experts meet one more time in a smaller circle. The task was to argue and negotiate new IMIDS structure that is acceptable for the private and public sector.

26.10.2018 final public-private workshop took place. Based on already agreed structure and with the help of outside moderator, experts worked in smaller groups. During the workshop, experts mapped relevant services and roles; identified challenges related with the services and offered possible solutions. In the end of December 2018, new draft version of the document was ready.

On February 15, 2019, EISA presented IMIDS to the e-Estonia Council who supported the identity management, eID and identity documents long-term plan [17].

After one and a half years of work, finally the identity management field had a starting point. Experts started to call the IMIDS as "white paper".

3.2 Process Outcome

IMIDS is a valuable set of area specific principles and guidelines and a starting point for the long-term visioning.

During the discussion experts found that term identity management is too broad, and they defined the document scope as follows:

- Identity of a person attributed by the state;
- Identity life cycle – all processes and activities;
- Identity management – management of data, tokens, Online Certificate Status Protocol (OCSP) service etc.;
- Usage - authentication, digital signature, encryption and decryption functionalities, eesti.ee e-mail address, NFC based services, biometrics;
- Ecosystem and cooperation – public vs private sector, research and development activities.

It means that the IMIDS focuses on the state created identities and does not deal with private sector identity solutions like Google or Facebook identities. Document covers the state created identity whole life cycle management and usage from the physical and electronic perspective.

During the process appeared that public and private sector experts understand and use professional terminology differently. For example, term "identity" had already various meanings and experts used it differently. Therefore, experts agreed most important definitions like identity document, identity carrier and carrier management, information service, clients etc. A separate glossary is a part of the document to increase the level of common understanding among public and private sector experts.

The document itself is twenty pages long and consist of five main chapters:

1. Market and Background (Estonia, EU, international level, service providers);
2. Predictable Future Developments;
3. National Identity Management Pillars and Principles;
4. Services Related to the Identity Management;
5. IMIDS Update Mechanisms.

First two chapters give general overview of the existing market situation and possible future trends on the state and international level. Next chapter is a set of

general principles and guidelines for the development activities. Fourth chapter is the core of IMIDS and reflects future development vision of identity management related services.

First chapter contains Estonian identity management and identity documents ecosystem brief overview and description of main players and their roles. Estonian identity management framework bases on four main pillars:

- Clients - physical persons, private and public sector entities;
- Identity carriers/tokens – all ID-1 format cards, eID, mobile-ID, smart-ID, travel documents/passports;
- Channels – service points, e-service portal, phone, development environment;
- Services – personal identification, confirmation of the will of the person, validity confirmation services, identity carrier management (including carrier recognition), information services, official e-mail address, development services, service support etc.

In addition to the Estonian identity environment overview, the chapter contains key points that influence and shape the European Union and international market. One interesting finding was that in past three/four years several international service providers in the security documents market have merged. For example, in 2015, Gemalto AG acquired Swiss company Trüb AG and currently Gemalto AG merger process with Thales Group is almost finished. In 2017, French company Morpho S.A.S merged with Oberthur Technologies currently named IDEMIA. This situation illustrates the consolidation of the technologies and competences and the decrease of competition on the international level.

Second chapter analyses possible future developments that affect identity management and identity documents field. Use of biometrics will be one of the key elements in next ten years. Countries experiment with different technologies and biometric identifiers (face, iris, behavioral features etc.). People dependency from the technology and relative importance of the mobile technologies increase. Smart cities become more popular and the block-chain field of application expands. Increasing IoT numbers cause data exchange overload. In the identity management area important developments in the field of machine learning, mathematical modelling of nervous systems and behavior predictability enable accurate identification from the pictures and videos. By 2035, airports have to be able to serve highly increased number of passengers.

Third chapter presents the identity management basic principles. Estonia is open for innovation and ready to pilot new technological solutions. On the other hand, state ensures readiness to cope with technological crisis and creates risk management plan with mitigation measures. To mitigate the risks the state prefers to purchase ID-1 format documents and travel documents from different companies. There is one central identity management database and state analyses possibilities how to offer identification service to the private sector. State wants to review and re-organize the current eID roles and work allocation. These were only some examples of the general principles.

Identity management and related services is a central part of the strategy. Experts pointed out under every service main challenges and directions. Personal identification service challenges are record keeping and access management, international cooperation, aging of the main information system, service availability, and unmanaged risks.

Experts offered solutions for facing these challenges. For example, finding way to process personal data outside of Estonia, implementing automatic biometrical identification system (ABIS), cooperating with international identity providers (GSMA, CITIC etc.).

Carrier management contains different aspects starting from issuance process to risk management. Identity documents application moves to the electronic environment and state engages private businesses in the identity document issuance process. State plans to implement Artificial Intelligence (AI) based solutions in the working processes and searches effective PKI independent and post-quantum solutions.

In the context of digital authentication and signing, state analyzes the possibility to use Estonian eID in international environments (Facebook, eBay, Google) and builds more services on the Near Field Communication (NFC) technology implemented on the new eID card starting from December 2018.

Identity systems developers need more support and attention. Experts suggested different solutions that help to cope with the changing technical environment. Usage of more standardized solutions is just one example.

IMIDS has no separate juridical power, but it will be an input to other political level strategical documents as Internal Security Development Plan (STAK) in the governing area of the Ministry of the Interior and Estonian Information Society Development Plan in the governing area of the Ministry of Economic Affairs and Communications.

According to the strategy document, public and private sector representatives meet once a year in the last quarter initiated by the PBGB and discuss if the document needs to be changed. The full text of the IMIDS is publicly available in Estonian on the PBGB and EISA web pages [3].

4 Important Findings and Discussions

4.1 General Organization

First part of the interviews focused on the IMIDS organizational side. As a warm-up question, we asked about the experience in the identity management field. All interviewees brought out approximate number of years they have worked in the area. Remarkable was the difference in experience between the private and public sector representatives. Public sector median experience in the area was 7.1 years and the same result in private sector was 19.28 years. It is quite remarkable difference and may be one of the reasons why two sectors have different views on the area.

All interviewees evaluated the necessity of the IMIDS on a ten-point scale, where one meant that the creation of the IMIDS was not relevant and ten referred that the strategy document was very necessary. Median score given by all interviewees was 8.92. Public sector median score was 8.8 and private sector score 9. Mainly, the interviewees said that real actions have to follow; otherwise, the strategy document has no practical value. In addition, it is not necessary to repeat already existing principles. Interviewees also marked that the importance was not only coming from the documented part but from the process itself. Experts had not meet to discuss area related

issues already long time. Therefore, it was a good opportunity to create mutual understanding among the public and private sector.

Interviewees had a chance to bring out positive and negative elements regarding the IMIDS creation process. The focus of the question was on the overall process structure, meetings held during the process, e-mail communication etc.

Interviewees found positive that the white paper finally created, and the community was around the table. They also pointed out that possibility to meet between private and public sector representatives in a smaller round was very helpful. All interviewees liked 26.10.2018 workshop moderated by professional.

Based on the received feedback it was clear that there is room for process improvement. Most important takeaways and findings are following:

- Engage professional methodical competence already to the strategy preparatory activities.
- Engage public and private sector representatives at the same time.
- Using iterative workshops format is most effective (as many iterations as needed).
- It is important to answer to all comments made during the process.
- Active participation and presence of ministries and policy makers level is very important.
- Interviewees pointed out that engaging the association level (ITL, Banking Association) was not sufficient.
- Telecommunication service providers (mobile operators), public sector IT houses (RMIT, KeMIT, TEHIK etc.) and experts from standardization authority were according to interviewees missing.
- Identity management and identity documents international level and industry view was missing.
- Too many people from the manager level participated.
- Too long periods between the meetings.

Time planning is another relevant issue in every project context. Therefore, we asked from the interviewees their opinion about the time actually spent (one and a half years). It was very interesting how interviewees' opinions about the IMIDS timeframe differed (the range was 3 months to 1.5 years). Most optimal duration seems to be up to six months. However, it is possible to make the document faster. The question is more about the optimal process planning.

4.2 Substantive Analysis

Last part of the interview concentrated on the IMIDS substantive analysis. During the IMIDS building process one of the questions that raised the debate was the juridical status of the document and on what level and by whom it should be approved. There is probably no right or wrong answer but based on the interviewee answers it is possible to fit the document better in the existing framework.

Most of the interviewees (46%) found that juridical status of the document is not necessary or important until the principles stated in the document adopt by the wider political documents like STAK and Information Society Development Plan. Others found that some kind of juridical or legal approval by the government or on the

ministry level is important to ensure the enforcement of the document. Others remained neutral or had no opinion about the topic.

Weather the document approved or not, more important is the actual enforcement of principles. The document is expression of expert opinions and the technical environment changes very fast; therefore, it is reasonable to keep the approval procedure rather simple and flexible. The maximum is ministry level, who can organize the introduction of the principles to the government and make the political selection from the IMIDS principles.

Currently PBGB and EISA led the IMIDS creation process. One of the interview questions was about the leadership of the project. Aim was to understand if this kind of dual leadership earned its purpose or are there any good alternatives. Opinions about the leadership were divergent. Interviewees who did not prefer concrete authority brought out that PBGB and EISA could both lead their area of competence separately. Then of course raises the question who will be responsible for putting together the overall picture. More important was the engagement of all related experts and authorities. To summarize this question, the leadership role can be on the ministry or implementation authority level, more important is involvement of the stakeholders and one responsible institution who coordinates the whole process.

In addition to concrete leadership issues, interviewees mentioned that there should be a centralized methodical competence center on a state level, assisting, guiding and advising the creation of similar expert level white papers. The idea is worth of considering if expert level white papers become more common in public sector.

Interviewees brought out following topics that should have been included to the IMIDS or presented more in detail:

- AI and machine learning development (how to use AI in different processes), because it brings lot of benefits and additional risks that need to be analyzed.
- Identity management of the things (AI-s, robots etc.).
- Risk management and related activities.
- Field of biometric solutions.
- Border crossing technical solutions (how to make border crossing faster and more convenient).
- International dimension representation. More specifically Estonian citizens in the international environment with tokens enabling the identification issued by Estonian public and private sector.
- Real actions planning part and input giving to the other implementation plans.

Strategy building and visioning is only one part of the whole picture, because after finalizing the strategy the real planning and work starts. Therefore, we asked from the interviewees how the IMIDS principles become reality. According to the answers, ministries should take a lead and integrate the principles coming from the IMIDS to STAK and ISDP. It was also emphasized that strong community and stakeholder's own attitude is very important, and all engaged parties should take the principles agreed in IMIDS account while planning future activities. One challenge in the implementation process is building up strong public and private partnership again.

Based on the answers it was possible to create a simplified model of the IMIDS implementation cycle. As first step interviewees found that it would be good to meet

shortly in a smaller group of public and private sector representatives, prioritize the actions, and select the most important issues that need urgent handling already during the year 2019. After prioritization, the experts have to describe a 10-step action plan and agree responsible authorities.

In the future, the meetings take place regularly once a year preferably in October or November. During these meetings, parties give an overview about implementing status and upcoming activities for the next and for the year after will be discussed (priorities and responsibilities overlooked or set, activities added or removed etc.). The reason for looking year and year after is the state budget planning principles that have direct influence on the implementation actions.

Close question to the previous one was how to keep the IMIDS document itself up to date. According to the document, experts overlook the IMIDS once a year initiated by the PBGB [3]. Interviewees approached to the question differently. Most of them found that need evaluation once a year is enough. Others found that evaluation shall happen more often or based on a necessity without any excessive administrative burden. They found that the focus should be more on flexibility and community-based interaction.

Based on the feedback we should consider CA/Browser Forum work format-based solution as an alternative. It is a strong and active expert community of certification authorities and Internet browser software vendors discussing and influencing international standards and principles [18]. The possibility to use similar format in Estonian identity management field for the public and private expert's cooperation needs further analysis. Therefore, current research is not concentrating to this particular topic in detail.

Two final questions were oriented to the main takeaways from the process and freely expressed comments if interviewees had any. As follows, we present only those takeaways and observations of the interviewees not already covered in the previous chapters:

- Some of the participants did not realize changed context – people who participated in the process were focusing too much to the historical context and did not realize that the situation is changed, and the same models are not applicable.
- Using the same terminology is important (i.e. the term "identity" is overwhelmed).
- Cooperation between the public and private cooperation has become very complex mainly because of the excessive regulatory environment and the feeling of unity is missing.
- Private sector was more active, interested and contributed more.
- Making this kind of white papers should be a common practice in public sector.
- Academic sector could be the bridge between different sectors.

Based on interviewee's answers to these two questions we noticed two main important conclusions. Firstly, interviewees mentioned multiple times that the cooperation between the public and private sector that once was much closer has become more reserved and complex. Mainly because of the too detailed regulatory framework (standards, laws, policies etc.). One of the solutions to overcome this situation offered during the interview was the engagement of academic sector who could be the bridge

between the public and private sector. This idea very interesting but of course the concept, format and readiness need separate analysis.

Secondly, interviewees suggested that the format of such white papers as IMIDS should be more widely used in public sector practice. It means that on the expert level in different areas the cooperation will become more active and documented. This wider view and its applicability need also more detailed analysis. As mentioned previously by one interviewee that in such cases there should be on a state level a methodical competence center who helps to guide the process and keeps track of different existing white papers and their changes.

4.3 Recommendations

Based on the analysis of the interviews and outcomes in combination with change management theory and approaches it is possible to design a model for the area specific long-term strategical documents.

The source of the initiative is not that important but usually it comes from the implementation authority who is working on the expert level on the specific area. As a first step, the implementation authority and responsible ministry shall meet and agree the division of labor, general principles and the list of involved stakeholders. After that, it is reasonable to engage methodical help. The role of the methodical help will be coordination and preparation of the meetings and workshops on a joint and smaller working group's level.

It would be good to have the first meeting jointly with public and private parties. The aim of the meeting is to introduce the initiative, agree main principles, work allocation, further steps and time schedule. In addition, the division of work between smaller working groups has to be agreed. Detailed work with concrete proposals shall continue in smaller working groups. The number of meetings in smaller working groups is not limited.

When the working groups are finished their discussions and formed their concrete proposals, the second joint meeting will take place. It is important to consider all proposals, negotiate if necessary and finally prioritize them. To have a systematic and uniform approach to the topic it would be good to use "why-what-how" technique for establishing a hierarchy for the expressed viewpoints [19]. If one meeting is not enough for that purpose, then it is possible to arrange more meetings until achieving mutual understanding and the public and private representatives confirm that the strategy is ready. After that, the document moves on the political level. The responsible ministry introduces the principles to the government, makes selection from the strategy taking into account the priorities, and integrates them in the political strategy document. Implementation actions will follow.

During the implementation, approximately once a year the implementation status and the principles agreed in the strategy will be gone through by the private and public sector representatives and changed if needed.

In addition to already above-mentioned aspects, it is important to keep in mind following principles:

- The whole process should not take more than six months;

- Uniform use of terminology shall be agreed in the beginning of the process;
- Continuous community building and public and private sector cooperation shall be happening as a parallel process;
- State shall provide centrally methodical help and relation management for sector specific strategies.

4.4 Future Direction

In the future, we would like to investigate the applicability of our findings internationally. Every country is different and therefore it is important to find universal aspects and make generalizations while investigating other mature e-countries. As a concrete next step, we will conduct a project with partners from the Netherlands, comparing the Estonian eID solution with cloud-based eID solution in the Netherlands with respect to eIDAS tiers.

5 Conclusion

Identity management and identity documents area is a complex system influencing almost invisibly different areas of life. Estonia as one of the leading e-countries has reached to the maturity level in terms of e-governance and it is crucial to think through the strategic next steps to bring innovation to the existing environment and retain competitive position on the international level.

Therefore, in the beginning of 2017 Estonian Police and Border Guard Board and Estonian Information System Authority initiated the strategy building process in the identity management area. After one and a half years of public and private sector stakeholder's meetings and workshops identity management white paper was finally ready.

Current article focus is on the previously named white paper building process analysis. The aim of the research was to find the answer to the main research question – how to design an effective long-term identity management strategy for a mature e-state. By using approach oriented towards action design research and based on qualitative individual structured non-standardized interviews in combination with theoretical framework, we proposed a model for building strategies on the identity management and identity documents field.

As strategy building is only one part of the change management process it is important that identity management and identity documents strategy does not remain on paper and implementation actions will follow in parallel with the public and private sector community building activities enabling one-step further as a mature e-state.

References

1. e-Estonia Briefing Centre Homepage. https://e-estonia.com/solutions/e-identity/id-card/. Accessed 21 Feb 2019

2. Laurent, M., Bouzefrane, S., Pomerol, J.: Digital Identity Management. ISTE Press, London (2015)
3. Identity Management and Identity Documents. White Paper 1.0. https://www.ria.ee/sites/default/files/content-editors/EID/valge-raamat-2018.pdf. Accessed 13 Mar 2019
4. Identity Documents Act. https://www.riigiteataja.ee/en/eli/526042018001/consolide. Accessed 13 Mar 2019
5. Peppard, J., Ward, J.: The Strategic Management of Information Systems, 4th edn. Wiley, Hoboken (2016)
6. Muldme, A., Pappel, I., Lauk, M., Draheim, D.: A survey on customer satisfaction in national electronic ID user support. In: Terán, L., Meier, A. (ed.) Piscataway 5th International Conference on eDemocracy & eGovernment (ICEDEG), Piscataway, NJ, Quito, pp. 31–37 (2018)
7. Petersson, A., Lundberg, J.: Applying action design research (ADR) to develop concept generation and selection methods. In: Wang, L., Kjellberg, T. (eds.) Procedia 26th CIRP Design Conference, vol. 50, pp. 222–227. Elseiver, Amsterdam (2016)
8. 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
9. Cameron, E., Green, M.: Making Sense of Change Management, 4th edn. Kogan Page Limited, London (2015)
10. Paide, K., Pappel, I., Vainsalu, H., Draheim, D.: On the systematic exploitation of the Estonian data exchange layer X-road for strengthening public private partnerships. In: Kankanhalli, A., Ojo, A., Soares, D. (eds.) 11th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2018, pp. 34–41. ACM Press, Galaway (2018)
11. Development Plans. https://www.valitsus.ee/et/eesmargid-tegevused/arengukavad. Accessed 24 Feb 2019
12. Internal Security Development Plan. https://www.valitsus.ee/sites/default/files/contenteditors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf. Accessed 13 Mar 2019
13. Estonian Information Society Development Plan. https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf. Accessed 25 Feb 2019
14. Järvsoo, M., Norta, A., Tsap, V., Pappel, I., Draheim, D.: Implementation of information security in the EU information systems. In: Al-Sharhan, S.A., et al. (eds.) I3E 2018. LNCS, vol. 11195, pp. 150–163. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02131-3_15
15. Electronic Identification and Trust Services for Electronic Transactions Act. https://www.riigiteataja.ee/en/eli/511012019010/consolide. Accessed 30 Mar 2019
16. 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
17. E-Eesti nõukogu toetas ID-kaardi ja eidentiteedi 10 aasta arenguplaani. https://www.ria.ee/et/uudised/e-eesti-noukogu-toetas-id-kaardi-ja-eidentiteedi-10-aasta-arenguplaani.html. Accessed 24 Feb 2019
18. CAB Forum Homepage. About the CA/Browser Forum - CAB Forum. https://cabforum.org/about-us/. Accessed 13 Mar 2019
19. APMG-international: Effective Change Manager's Handbook - Essential guidance to the change management body of knowledge, 1st ed. Kogan Page Limited, London (2015)

Appendix 6

VI
S. Lips, I. Pappel, V. Tsap, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In *the 7th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2018, pages 60–70, 2018

Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field

Silvia Lips[1], Ingrid Pappel[2], Valentyna Tsap[2], and Dirk Draheim[2( )]

[1] Politsei, Pärnu mnt. 139, 15060 Tallinn, Estonia
silvia.lips@politsei.ee
[2] Large-Scale Systems Group, Tallinn University of Technology, Akadeemia tee 15a, 12618 Tallinn, Estonia
{ingrid.pappel,valentyna.tsap,dirk.draheim}@ttu.ee

Abstract. In 2017, the encryption vulnerability of a widespread chip led to major, nation-wide eID card incidents in several EU countries. In this paper, we investigate the Estonian case. We start with an analysis of the Estonian eID field in terms of stakeholders and their responsibilities. Then, we describe the incident management from the inside perspective of the crisis management team, covering the whole incident timeline (including issues in response, continuity and recovery). From this, we are able to derive key factors in coping with large-scale security vulnerabilities in the eID field (public-private partnership, technical factors, crisis management, documentation), which encourages further research and systematization.

Keywords: e-identity · e-governance · e-services · IT security
Crisis management · Business continuity management

1 Introduction

Since the 1990s, Estonia was one of those republics that rapidly developed a priority on ICT. Since then, year by year, the country has shown a remarkable progress in building up elements and components of today's digital society. In particular, this regards the area of eID (electronic identity) management, which is a crucial enabler for the digital society. First eID cards were issued as early as in 2002, becoming mandatory documents. A full replacement with the new standard ID card has finished in 2006, and simultaneously, the state set up the required infrastructure for the entire e-services system. In these endeavors, public-private partnership turned out to be a winning model that ensured further smooth implementation, rollout and up-take of eID. Throughout all the time, based on continuous improvement of its public services and their delivery, Estonia has gained its citizens' trust. The matter of security (and trust) has always been and remains one of the top requirements in this area.

In 2017, Estonia encountered a nation-wide, urgent e-identity security issue: a potential encryption vulnerability of the chips used in current eID cards has

A. Kő and E. Francesconi (Eds.): EGOVIS 2018, LNCS 11032, pp. 60–70, 2018.
https://doi.org/10.1007/978-3-319-98349-3_5

been encountered and reported by Check and Slovak researchers. This paper provides in-depth description of the incident and the steps taken by the government authorities towards solving this crisis.

In Sect. 2 we will describe the Estonian eID ecosystem components. In Sect. 3, we will delve into the scope of the discovered security vulnerability, including its technical aspect and Estonia's approach of dealing with the occurred situation. In Sect. 4, we will identify the key factors in coping with the security crisis. We will finish the paper with a conclusion in Sect. 5.

2 The Estonian eID Ecosystem

Electronic ID and electronic signature are crucial building blocks in any serious e-government initiative, compare, e.g., with [1,2]. In this section, we will describe the Estonian eID ecosystem. Before we can analyze the factors in coping with large-scale security vulnerabilities, it is important to understand how the entire system works; who the main stakeholders are; what kind of eID tokens are used; and what role and influence the eID field has in the context of Estonian e-governance and electronic services.

2.1 Estonian eID Scheme Stakeholders

The Estonian eID ecosystem [3,4] is a unique and well-operating network consisting of different players and roles. Main authorities in the scheme (Fig. 1) are the Estonian Police and Border Guard Board (PBGB) and the Information System Authority (RIA).

- RIA operates in the governing area of the Ministry of Economic Affairs and Communications[1]. It coordinates the development and administration of the state's information system, organizes activities related to information security, coordinates the functioning of the public key infrastructure and handles security incidents that occur in Estonian computer networks[2]. In general, it can be said that RIA is the eID technical competence center.
- PBGB operates in the governing area of the Ministry of the Interior and is responsible for the identity management and the issuance of identity documents. This authority holds, manages and procures contracts necessary for keeping up the eID scheme (eID carriers, personalization service, certification service etc.). Current partner regarding the ID-1 format documents is a French security company Gemalto AG[3].
- Gemalto AG (via the associated company Trüb Baltic AS) manufactures and personalizes the eID cards and provides certification service (trust service) using SK ID Solutions AS as a sub-contractor.

[1] https://www.mkm.ee/en.
[2] https://www.ria.ee/en/.
[3] https://www.gemalto.com/.

Fig. 1. Estonian eID main stakeholders

- The ICT and development center (SMIT)[4] offers different ICT services (management and development of information systems, technical support etc.) in the whole internal security area under the Ministry of Interior.

In addition to the above-mentioned organizations, the Ministry of Foreign Affairs[5] issues identity documents and is responsible for diplomatic documents. The Technical Regulatory Authority (TJA)[6] has a supervisory role over the trust service providers [5]. Banks are e-service providers in the eID environment. Furthermore, some banks offer PIN-replacement services for eID cards.

2.2 Estonian eID Tokens

The ID-card is a mandatory identity document for citizens of Estonia enabling electronic authentication and qualified electronic signature [6] according to the eIDAS regulation [7]. The same type of card is issued to the European Union citizens residing in Estonia [8]. In addition to the ID-card there are many different eID tokens with the same electronic functionalities available:

1. Residence permit cards – issued to the third country nationals and persons with undetermined citizenship [9].
2. Digital identity cards (including e-residency cards) – voluntary secondary document for digital use only.

[4] https://www.smit.ee/.
[5] http://vm.ee/en.
[6] https://www.tja.ee/en.

3. Diplomatic identity cards – cards with full eID functionality issued by Estonian Ministry of Foreign Affair for diplomatic purposes.

As a convenient alternative to the card format, mobile IDs can be used. All of the available eID tokens enable electronic authentication and qualified electronic signature according to the eIDAS regulation.

With this wide variety of eID tokens the state has ensured access to e-services on equal basis to all interest groups. In addition to the authentication and signing solutions that are provided by the state, there are several other options available provided by private sector entities (e.g. bank links, smart-IDs, pin calculators etc.).

2.3 The Role of eID in e-Governance and e-Services

The usage of eID in Estonia is relatively high. 98% of Estonians have ID-cards and about 2/3 of the holders use their card regularly[7]. This means that the usage of e-services is remarkably high and the role of e-governance in the country is crucial.

According to [10], 99% of bank transfers in Estonia are made electronically, 98% of tax returns are made via the e-Tax board, 95% of prescribed medications are bought using digital prescriptions, etc. From the government perspective the state portal eesti.ee acts as single point of contact to the e-services offered by the state – ranging from health and medical related services to services in the area of business and entrepreneurship[8]. The total number of e-services in the country offered by public and private sector is around 2000.

The state portal eesti.ee is a gate to the Estonian e-state. The eID serves as a key that enables a secure access to all public and private e-services. This explains the vital role and importance of the eID in Estonia.

3 About Security Vulnerability

On the 30th of August 2017 RIA was informed about a potential security vulnerability in the Estonian eID card chips. The vulnerability was discovered by Slovak and Czech scientist during their research regarding RSA key generation and reported in [11]. At that time, it was not clear what number of cards is actually affected. This section gives an overview about the nature and scope of the security vulnerability and how it was handled.

3.1 Technical Description and Scope of the Security Vulnerability

In [11,12] it has been reported that a wide range of cryptographic chips produced by Infineon Technologies AG are vulnerable with respect to RSA (Rivest-Shamir-Adleman) key pair generation. One of those chips is implemented in Estonian

[7] https://e-estonia.com/solutions/e-identity/id-card/.
[8] https://www.eesti.ee/en/.

eID cards starting from October 2014. As a result of the chip's vulnerability, it became possible to calculate the RSA private key of an eID card holder with the knowledge of the corresponding RSA public key with critically less computational complexity than should be expected from properly implemented RSA system. As a consequence, all Estonian eID cards issued after 16.10.2014 were potentially vulnerable – in total about 750.000 issued cards with full eID functionality. This was about 2/3 of all issued cards (ID cards, residence permit cards, digital identity cards including e-residency cards). The mobile ID solution used by about 70.000 users was not affected due to its different technical solution.

Based on these numbers and the users' high dependence of the eID-based services, it can be said that the state had to deal with a very sensitive and large-scale security issue. Hence, a solution had to be implemented rapidly and at the same time, all possible risks and consequences had to be acknowledged by the parties that were involved into the crisis handling.

3.2 Process of Handling the Security Vulnerability in Estonia

After receiving the information about the vulnerability, RIA convened a roundtable of experts to prepare preliminary directions for a solution and communication. Technical and communication working groups worked in parallel. Results of the both working groups were presented to the government.

It was the first time that the state faced such a large-scale security topic in the eID field and the government decided to take an open approach and discuss the issue veraciously. The main reason for this was to retain trust towards e-solutions and e-governance. The crisis management was delegated to RIA and PBGB (Fig. 2).

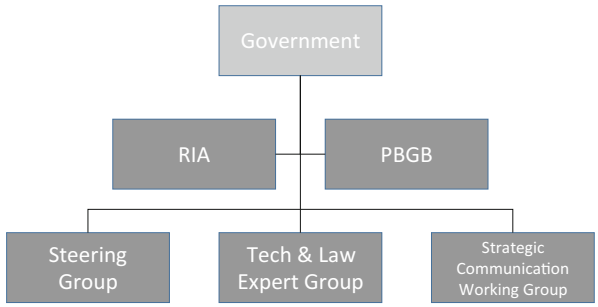

Fig. 2. Delegation of crisis management during the 2017 Estonian eID card incident.

In both organizations (RIA and PBGB), crisis managers were entitled. Under the management of RIA, a steering group of managers of involved authorities met regularly. At least two times a week working group of technical and law experts met to present latest findings and improvements and negotiate technical nuances.

As the vulnerability concerned the majority of the eID users, communication played a decisive role in the whole process. The main challenge was to explain the technically complex topic in a simple and understandable way in order to avoid general panic and to give clear guidelines. Therefore, in parallel to seeking for a technical solution, a group of communication experts from the different authorities dealt with strategical communication matters.

As a preventive measure, access to the LDAP (Lightweight Directory Access Protocol) catalogue service for certificate status requests has been limited. The access to the service has been limited to authorized entities to prevent uncontrolled downloads from the eID card users public key database. (after the successful recovery from the incident, the service was opened again on 20.11.2017).

The technical working group concluded that the best way to solve the security issue is to implement elliptic curve cryptography (ECC) in eID documents. This decision led to three types of development works:

1. With respect to new cards: adjustments of the eID card production capacities to implement ECC and to ensure readiness to personalize new cards;
2. 1. With respect to 750.000 already issued cards: update of already existing software enabling a certificate renewal procedure
   (a) in PBGB service points (the document holder can come to a PBGB service point and an official will renew certificates on site).
   (b) in document holder's personal computer (the document holder can renew his/her certificates remotely on his/her PC).

The renewal process started in the end of October 2017, after adjustments to the eID cards production had been implemented. In the beginning of November, all certificates were suspended in order to avoid possible damage. Therefore, it became impossible to use them in the e-environment unless renewed. With renewed certificates, eID cards could be used as usual. Starting from April 2018, the suspended certificates will be revoked and renewal will not be possible anymore, and therefore, those eID holders who did not renew it by that time will have to apply for a new document in case they want to use it in the e-environment.

3.3 Positive and Negative Effects of the Vulnerability

When it comes to occurrence of similar incidents, negative and positive aspects can be identified and used for further consideration and analysis of problem solving. At this moment, the aspects presented below are identified.

At the negative side:

- Debate regarding accountability – accountability is usually a matter that needs to be clarified during the process; but very often it is not the easiest part. These legal ongoing debates are tiring and expensive.
- Media pressure and noise – the number of people working in eID field in Estonia is rather limited. In some cases, the media pressure was quite intensive and started even to disturb experts' work.

- Some crucial functionality was temporarily lost - to resolve the security issue quickly, this had to be accepted. The Estonian eID card has an encryption functionality that was not possible to develop as fast as needed. As a consequence, in the new secure eID cards with ECC the encryption function was temporarily missing. This influenced majorly those users who used this functionality for secure document transmission (including many public sector authorities).
- Other ongoing activities were set on a hold – eID experts worked about 5 months to solve the security issue and various important projects were set on a hold until the end of the crisis.

At the positive side:

- Raised eID awareness – the eID field was in media from different angles almost every day during the active crisis period from September to December 2017. The case was published and analyzed publicly in detail. The awareness about eID functionality and use cases was definitely raised.
- Raised security awareness – in addition to eID awareness, the security awareness improved. The real case in the security field encouraged different security related debates in society.
- Stronger public and private cooperation – when the vulnerability was discovered all public and private authorities started to offer their help to the mainly involved authorities. The private sector was ready to contribute in any way to solve the issue as fast as possible. After this experience, it was clear that in complex situations the cooperation between public and private sector is very advantageous.
- Improved crisis management readiness – after dealing with concrete crisis and analyzing the results it was possible to make general conclusions and improve the existing crisis management system where needed.

3.4 How Other Affected States Coped with the Vulnerability

In addition to Estonia, Slovakia, Austria and Spain faced the same security vulnerability. Austria was the first country who reworked all its eID certificates on 09.06.2017 and informed other EU member states about it. CERT Estonia, which is a unit under the RIA responsible for the security incident management in the country, received this information on 20.06.2017. As the number of the certificates revoked by Austria was only few thousand, it did not have large scale impact in the country.

On 23.10.2017, the Ministry of Interior of Slovakia officially informed about suspension of the qualified electronic signature certificates on Slovak eID cards [13]. Both countries, Slovakia and Estonia suspended their certificates at about the same time. According to the information received from RIA, in the Slovakian case about 300.000 eID cards were affected.

The Spain case may seem to be the most interesting one. In the middle of November 2017, it was still not clear how Spain is going to handle the security

vulnerability and no communication was made [14]. There is around 60 million eID cards on the market but according to RIA information, not all of them were affected. All certificates of the potentially vulnerable eID cards were finally suspended (more than 10 million) [15]. Despite of a huge number of suspended certificates, the overall effect in the country was not remarkable as the usage of eID in Spain is very low.

4 Key Factors in Coping with the Estonian eID Crisis

This section is oriented towards the main factors that played a key role while solving the Estonian eID crisis and towards the lessons learned from positive and negative perspectives on it. In each crisis situation, there is a vast amount of different aspects and probably, no single correct recipe or way to solve it. However, some key factors that help to cope with the situation more easily or to prevent even bigger damage can be identified. In the Estonian case we found that public-private partnership, technical solutions in use, crisis management, and communication are crucial factors.

4.1 Public-Private Partnership

In case of large-scale security vulnerabilities, there is no certain way of handling it and necessary competences range from ICT developers and security experts to communication specialist. Therefore, it might not be reasonable for a country to employ these competences permanently. More preferable is to have a good and supportive expert network that can be engaged if needed.

In the Estonian case, the PPP (public-private partnership) [16] performed very well and all public and private sector stakeholders and interested parties made their contribution. A specific expertise and resources were made available for public use. The small size of Estonia may play a role here, yet professional communities in the eID field are usually quite small everywhere. Therefore, the Estonian case might be considered as a good example of how PPP works effectively.

4.2 Technical Success Factors

From a technical point of view, the existence of an alternative eID token was crucial. Mobile ID was the only token that was not affected by the security vulnerability. People who already had it did not have to worry about their eID card status and further use of e-services. People who did not yet have mobile ID could apply for it easily and keep using e-services.

The other key factor was the *availability of an alternative renewal solution* after enabling a modified certification renewal process. It was possible to renew certificates in the PBGB service points as well as remotely on a user's PC. The renewal solution helped to save already issued eID cards and people had alternatives to choose from. Furthermore, the remote update solution helped to prevent an overloading of the PBGB service points.

4.3 Crisis Management

It was highly beneficial that a single authority (RIA) was responsible for the overall coordination from start to end. RIA acted as a single point of contact and the entire flow of important information needed for making strategic decisions was managed centrally. Using special expert level working groups simplified the work and enabled the discussion and weighting of various alternative solutions before the selection of the final one.

The *project-based management* used in the Estonian case can be considered as a success story. Different alternative project plans were put together taking into account instable and changing circumstances. Depending on the situation, plans were easy to exchangeable and to use. The public sector is usually considered more conservative and rather slowly changing. The Estonia eID crisis showed that it is possible to implement new approaches very fast. The state made a step closer to the users and opened extra temporary service points for renewal in hospitals, bigger shopping centers etc., which not only provided more options to citizens but also allowed to avoid overloading of PBGB service points.

4.4 Documentation and Verification

In a crisis situation, a need for juridical interpretation of state and European Union legal acts and contract clauses has occurred often. Therefore, *having lawyers and legal advisors in the technical working group* already in the early stage of the crisis was essential. Even if the timeframes were strict, a new *technical solution* has yet to be verified, audited, or reviewed before going live in order to prevent further mistakes or creating new security weaknesses. The adjustment of Estonian eID cards production capacities was verified and, changes in software were reviewed by independent third parties. After the crisis RIA ordered an *overall study* on how the eID crisis was managed inside the country, what were the main lessons learned and what can be improved. The study will be based on qualitative interviews with managers, experts and specialist who participated in the crisis settlement. On the basis of this, we suggest to turn the experience gathered during this incident into a rigorous, formal continuity management process [17–20].

5 Conclusion

The discovered RSA key vulnerability can be seen as one of those numerous risks that should be expected when it comes to technologies that a state's functionality so strongly relies on. Estonian experience with encountering a security issue that is a potential threat to country's now fundamental components demonstrates a rather strong and vigorous approach. The government has promptly reacted once the issue was announced convening all engaged stakeholders and experts allowing for solving the problem as fast as possible, taking into account carefully the associated risks and scenarios notwithstanding the urgency.

It is important to bear in mind here that regardless of how reliable and complex a technical solution can be, its reliability remains relative [21]. Every system, hardware or software is vulnerable to unknown attacks and there is no way of keeping this so-called status quo when we define a solution to be secure. A plausible conjecture that can be put here, based on what was said above, is for those in charge to take into account the risks of occurrence of similar threats and invest sufficient resources into retaining possible suitable auxiliaries for problem-solving if such events take place. The lessons learned that we outlined in this paper are generalized conclusions which derive from studying and analyzing this incident that happened recently, therefore we are aiming to extend them further once a more detailed and in-depth research will be conducted after collecting additional data and insights from stakeholders.

Hence, we are convinced that the Estonian practice of handling the e-identity security issue crisis is a decent example and a result of an effective and agile management, which relied heavily on public-private partnership, openness, technological advances of the country and continuous reviews and analysis of performance.

References

1. Marsalek, A., Zefferer, T., Reimair, F., Karabat, Ç., Soykan, E.U.: Leveraging the adoption of electronic identities and electronic-signature solutions in Europe. In: Proceedings of the Symposium on Applied Computing, SAC 2017, pp. 69–71. ACM, New York (2017)
2. Luna-Reyes, L.F., Sandoval-Almazan, R., Puron-Cid, G., Picazo-Vela, S., Luna, D.E., Gil-Garcia, J.R.: Understanding public value creation in the delivery of electronic services. In: Janssen, M., et al. (eds.) EGOV 2017. LNCS, vol. 10428, pp. 378–385. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64677-0_31
3. Muldme, A., Pappel, I., Lauk, M., Draheim, D.: A survey on customer satisfaction in national electronic ID user support. In: 2018 International Conference on eDemocracy eGovernment (ICEDEG), pp. 31–37, April 2018
4. 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
5. Republic of Estonia: Electronic identification and trust services for electronic transactions act. https://www.riigiteataja.ee/en/eli/527102016001/
6. 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
7. European Union: Regulation (EU) no. 910/2014 of the European Parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC (2014)
8. Republic of Estonia: Identity documents act. https://www.riigiteataja.ee/en/eli/521062017003/

9. Republic of Estonia: Aliens act. https://www.riigiteataja.ee/en/eli/501112017003/
10. E-Governance Adacemy: e-Estonia - e-governance in practice. eGA, Tallinn (2016). https://goo.gl/JfpwNN
11. Nemec, M., Sys, M., Svenda, P., Klinec, D., Matyas, V.: The return of coppersmith's attack: practical factorization of widely used RSA moduli. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pp. 1631–1648. ACM, New York (2017)
12. Svenda, P., et al.: The million-key question - investigating the origins of RSA public keys. In: 25th USENIX Security Symposium, pp. 893–910. USENIX Association (2017)
13. První certifikační autorita: Safety of starcos cards. I.CA News Feed, November 2017. http://www.ica.cz/News?IdNews=363
14. Meyer, D.: ID card security - Spain is facing chaos over chip crypto flaws. ZDNet, November 2017. https://goo.gl/8xWizW
15. Leyden, J.: Confusion reigns over crypto vuln in Spanish electronic ID smartcards - certs revoked, but where are the updates? The register, November 2017
16. Paide, K., Pappel, I., Vainsalu, H., Draheim, D.: On the systematic exploitation of the Estonian data exchange layer X-road for strengthening public private partnerships. In: 11th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2018. ACM (2018)
17. British Standards Institution: Business continuity management - part 1: code of practice, British Standard BS 259991:2006. BSI Group, London (2006)
18. British Standards Institution: Societal security - business continuity management systems - requirements. BSI Group, London (2014)
19. Draheim, D.: Smart business process management. In: 2011 BPM and Workflow Handbook, Digital Edition. Future Strategies, Workflow Management Coalition, pp. 207–223 (2012)
20. Draheim, D., Pirinen, R.: Towards exploiting social software for business continuity management. In: Workshops on Database and Expert Systems Applications (DEXA), pp. 279–283. IEEE Press, September 2011
21. Buldas, A., Saarepera, M.: Are the current system engineering practices sufficient to meet cyber crime? In: Tryfonas, T. (ed.) HAS 2017. LNCS, vol. 10292, pp. 451–463. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-58460-7_31

Curriculum Vitae

1. Personal data

Name	Silvia Lips
Date and place of birth	22 March 1984 Viljandi, Estonia
Nationality	Estonian

2. Contact information

Address	Tallinn University of Technology, School of Information Technologies, Department of Software Science, Ehitajate tee 5, 19086 Tallinn, Estonia
Phone	+372 55 26 116
E-mail	silvia.lips@taltech.ee

3. Education

2018–...	Tallinn University of Technology, School of Information Technology, PhD studies
2012–2019	Tallinn University of Technology, School of Information Technology, e-Governance technologies and services, MSc *cum laude*
2004–2006	Tallinn University (former University Nord), Faculty of Law, Law, LL.M *cum laude*
2001–2004	Tallinn University (former University Nord), Faculty of Law, Law, BSc *cum laude*

4. Language competence

Estonian	native
English	fluent
Russian	intermediate
German	beginner
French	beginner

5. Professional employment

2021– ...	Information System Authority, Expert/eIDAS SPOC
2019– ...	Tallinn University of Technology, Early Stage Researcher
2019–2019	Police and Border Guard Board, ePassport project consultant
2014–2019	Police and Border Guard Board, Adviser-Expert
2009–2014	IT and Development Centre. Ministry of the Interior, Estonia (SMIT), Head of Legal and Procurement Department
2008–2009	IT and Development Centre. Ministry of the Interior, Estonia (SMIT), Leading Expert on Legal Affairs
2007–2008	Citizenship and Migration Board Estonia, Leading Specialist of Legal Department
2006–2007	Citizenship and Migration Board Estonia, Chief Specialist of Legal Department
2004–2006	Estonian Academy of Security Sciences, Legal training manager

6. Voluntary work

2005–2006 Estonian Animal Protection Association, voluntary lawyer

7. Projects

2020–2021	A Digital Infrastructure for Cross Border e-Commerce (SaaS), project manager
2019–2020	Tender for e-Commerce EU VAT and Duty Declaration (as from 2021) Digitalization, legal environment analyst

8. Supervision

- Stina Mander, Master's Degree, 2023, (sup) Silvia Lips, The Utilization of Public-Private Partnership (PPP) Framework in the Management of eID Projects, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Isaac Obeng-Anyan, Master's Degree, 2023, (sup) Silvia Lips, Leveraging the Digital Credentials of the Ghanaian eID to Streamline Healthcare in Ghana, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Urfan Mahyaddinova, Master's Degree, 2023, (sup) Silvia Lips, Increasing the Use of ASAN Signature in the E-government Services in Azerbaijan, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Jaanus Riibe, Master's Degree, 2023, (sup) Silvia Lips, Improving Crisis Communication Management at the Local Municipalities: an e-Service Proposal, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Karolina Bejussova, Master's Degree, 2022, (sup) Silvia Lips, Assessment of the eID Ecosystem as a Part of the State's Critical Infrastructure: the Case of Estonia, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Mahabubul Hasan, Master's Degree, 2021, (sup) Silvia Lips, Managing and Tracking e-Health Data Using Smart ID-Card in Bangladesh, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Helen Raamat, Master's Degree, 2021, (sup) Innar Liiv; Silvia Lips, Estonian Digital Public Service Improvement Analysis in Cross-Border Use Cases, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Ruslan Kononov, Master's Degree, 2021, (sup) Sadok Ben Yahia; Silvia Lips, Evaluation of Facial Emotion Recognition Models for the Potential Deployment in Web-based Learning Environments, Tallinn University of Technology School of Information Technologies, Department of Software Science
- Natalia Vinogradova, Master's Degree, 2021, (sup) Silvia Lips, Re-Shaping the eIDAS Regulation from Stakeholders Perspective, Tallinn University of Technology School of Information Technologies, Department of Software Science

- Mohammed Saber Hafez Abdelhafis Sallam, Master's Degree, 2021, (sup) Silvia Lips, Success and Success Factors of the Estonian e-Residency from State and Entrepreneurs Perspective, Tallinn University of Technology School of Information Technologies, Department of Software Science

- Oladele Solomon Amola, Master's Degree, 2021, (sup) Silvia Lips, Designing Crisis Management Mobile Application: a Case Study of Lagos State in Nigeria, Tallinn University of Technology School of Information Technologies, Department of Software Science

- Jose Ernesto Cueto Morales, Master's Degree, 2020, (sup) Silvia Lips, Improving the Digital Identity Management System in Mexico, Tallinn University of Technology School of Information Technologies, Department of Software Science

- Khayyam Zulfigarzada, Master's Degree, 2020, (sup) Silvia Lips, Designing Government e-Petition System in Azerbaijan, Tallinn University of Technology School of Information Technologies, Department of Software Science

- Syed Mohsin Raza Naqvi, Master's Degree, 2020, (sup) Silvia Lips; Sidra Azmat Butt, Challenges and Opportunities of Applying e-ID (Smart National Identity Card) in Public Sector of Pakistan, Tallinn University of Technology School of Information Technologies, Department of Software Science

9. Defended theses

- 2019, "Designing an Effective Long-Term Identity Management Strategy for a Mature e-State", MSc, supervisor Prof. Dirk Draheim, co-supervisor Assoc. Prof. Ingrid Pappel, Tallinn University of Technology, Department of Software Science

- 2006, "The aspects of the biometrical identification and verification through the data protection law", LL.M, supervisor LL.M Rainer Osanik, co-supervisor MA Veiko Kopamees, Tallinn University, Faculty of Law, Department of Civil and Commercial Law

- 2004, "Comparative and Legal Analysis of Estonian and English Insurance Law", BSc, supervisor LL.M Rainer Osanik, Tallinn University, Faculty of Law, Department of Civil and Commercial Law

10. Field of research

- 4.6. Computer Science

- 4.7. Information and Communications Technologies

11. Scientific work
Papers

1. S. Lips, V. Tsap, N. Bharosa, R. Krimmer, D. Draheim, and T. Tammet. Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia. In *Information Systems Frontiers*, 2023

2. R. K. Ahmed, M. H. Khder, S. Lips, K. Nyman-Metcalf, I. Pappel, and D. Draheim. A Legal Framework for Digital Transformation. *International Journal of Electronic Government Research (IJEGR)*, XXXX

Conference presentations

1. M. S. H. A. Sallam, S. Lips, and D. Draheim. Success and success factors of the Estonian e-residency from the state and entrepreneur perspective. In *the 8th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2021, pages 291–304, Cham, 2022. Springer

2. S. Lips, N. Vinogradova, R. Krimmer, and D. Draheim. Re-shaping the EU digital identity framework. In *the 23rd Annual International Conference on Digital Government Research*, dg.o 2022, page 13–21, New York, NY, USA, 2022. Association for Computing Machinery

3. S. Lips, R. K. Ahmed, K. Zulfigarzada, R. Krimmer, and D. Draheim. Digital sovereignty and participation in an autocratic state: Designing an e-petition system for developing countries. In *the 22nd Annual International Conference on Digital Government Research*, dg.o 21, page 123–131, New York, NY, USA, 2021. Association for Computing Machinery

4. 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 *the 10th International Conference Electronic Government and the Information Systems Perspective*, *EGOVIS 2021*, volume 12926 of *Lecture Notes in Computer Science*, pages 73–85, Cham, 2021. Springer

5. R. K. Ahmed, K. H. Muhammed, A. O. Qadir, S. I. Arif, S. Lips, K. Nyman-Metcalf, I. Pappel, and D. Draheim. A legal framework for digital transformation: A proposal based on a comparative case study. In *the 10th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2021, pages 115–128, Cham, 2021. Springer

6. O. Amola, S. Lips, and D. Draheim. *Designing a Crisis Management Mobile Application Solution in Nigeria*, page 571–579. Association for Computing Machinery, New York, NY, USA, 2021

7. R. Saputro, I. Pappel, H. Vainsalu, S. Lips, and D. Draheim. Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study. In *the 7th International Conference on eDemocracy & eGovernment*, *ICEDEG 2020*, pages 216–222, 2020

8. V. Tsap, S. Lips, and D. Draheim. Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In *the 9th International Conference on Electronic Government and the Information Systems Perspective*, *EGOVIS 2020*, volume 12394 of *Lecture Notes in Computer Science*, pages 159–173, Cham, 2020. Springer

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

10. R. K. Ahmed, S. Lips, and D. Draheim. eSignature in eCourt systems. In *2020 Fourth World Conference on Smart Trends in Systems*, *Security and Sustainability (WorldS4)*, pages 352–356. IEEE, 2020

11. 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, *Electronic Participation*, pages 41–53, Cham, 2020. Springer

12. S. Lips, N. Bharosa, and D. Draheim. eIDAS implementation challenges: the case of Estonia and the Netherlands. In *the 7th International Conference on Electronic Governance and Open Society: Challenges in Eurasia*, EGOSE 2020, pages 75–89, 2020

13. S. Lips, K. Aas, I. Pappel, and D. Draheim. Designing an effective long-term identity management strategy for a mature e-state. In *the 8th Electronic Government and the Information Systems Perspective*, EGOVIS 2019, pages 221–234, Cham, 2019. Springer

14. S. Lips, I. Pappel, V. Tsap, and D. Draheim. Key factors in coping with large-scale security vulnerabilities in the eID field. In *the 7th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2018, pages 60–70, 2018

15. S. A. Butt, S. Lips, R. Sharma, I. Pappel, and D. Draheim. Barriers to digital transformation of the silver economy: Challenges to adopting digital skills by the silver generation. In *the 14th International Conference on Applied Human Factors and Ergonomics*, AHFE 2023. Springer, 2023

16. S. Mander, S. Lips, and D. Draheim. The utilization of public-private partnership frameworks in the management of eid projects. In *the 12th International Conference on Electronic Government and the Information Systems Perspective*, EGOVIS 2023. Springer, 2023

Elulookirjeldus

1. Isikuandmed

Nimi	Silvia Lips
Sünniaeg ja -koht	22.03.1984, Viljandi, Eesti
Kodakondsus	Eesti

2. Kontaktandmed

Aadress	Tallinna Tehnikaülikool, Tarkvarateaduste Instituut, Ehitajate tee 5, 19086 Tallinn, Estonia
Telefon	+372 55 26 116
E-post	silvia.lips@taltech.ee

3. Haridus

2018–…	Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, doktoriõpe
2012–2019	Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, e-Riigi tehnoloogiad ja teenused, MSc *cum laude*
2004–2006	Tallinna Ülikool (end. Akadeemia Nord), Õigusteaduskond, õigusteadus, LL.M *cum laude*
2001–2004	Tallinna Ülikool (end. Akadeemia Nord), Õigusteaduskond, õigusteadus, BSc *cum laude*

4. Keelteoskus

eesti keel	emakeel
inglise keel	kõrgtase
vene keel	kesktase
saksa keel	algtase
prantsuse keel	algtase

5. Teenistuskäik

2021– …	Riigi Infosüsteemi Amet, ekspert/eIDAS ühtne kontaktpunkt
2019– …	Tallinna Tehnikaülikool, nooremteadur
2019–2019	Politsei- ja Piirivalveamet, e-passi projekti konsultant
2014–2019	Politsei- ja Piirivalveamet, nõunik-ekspert
2009–2014	Siseministeeriumi infotehnoloogia- ja arenduskeskus, õigus- ja hankeosakonna juhataja
2008–2009	Siseministeeriumi infotehnoloogia- ja arenduskeskus, õiguse juhtiveksper
2007–2008	Kodakondsus- ja Migratsiooniamet, õigusosakonna juhtivspetsialist
2006–2007	Kodakondsus- ja Migratsiooniamet, õigusosakonna peaspetsialist
2004–2006	Sisekaitseakadeemia, õiguskoolitusjuht

6. Vabatahtlik töö

2005–2006	Eesti Loomakaitse Selts, vabatahtlik jurist

7. Projektid

2020–2021	Digitaalne infrastruktuur piiriüleseks e-kaubanduseks, projektijuht
2019–2020	E-kaubanduse EL käibemaksu- ja tollideklaratsioonide (alates 2021. aastast) digitaliseerimine, õiguskeskkonna analüütik

8. Juhendatud väitekirjad

- Stina Mander, magistrikraad, 2023, (sup) Silvia Lips, The Utilization of Public-Private Partnership (PPP) Framework in the Management of eID Projects (Avaliku ja erasektori partnerluse (PPP) raamistiku kasutamine eID projektide juhtimisel), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Isaac Obeng-Anyan, magistrikraad, 2023, (sup) Silvia Lips, Leveraging the Digital Credentials of the Ghanaian eID to Streamline Healthcare in Ghana (Ghana eID digitaalsete andmete kasutamine tervishoiuteenuste sujuvamaks pakkumiseks Ghanas), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Urfan Mahyaddinova, magistrikraad, 2023, (sup) Silvia Lips, Increasing the Use of ASAN Signature in the E-government Services in Azerbaijan (ASAN-allkirja kasutamise suurendamine e-valitsuse teenustes Aserbaidžaanis), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Jaanus Riibe, magistrikraad, 2023, (juh) Silvia Lips, Improving Crisis Communication Management at the Local Municipalities: an e-Service Proposal (Kriisikommunikatsiooni juhtimise täiustamine kohalikes omavalitsustes: e-teenuse ettepanek), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Karolina Bejussova, magistrikraad, 2022, (juh) Silvia Lips, Assessment of the eID Ecosystem as a Part of the State‘s Critical Infrastructure: the Case of Estonia (eID ökosüsteemi kui riigi kriitilise infrastruktuuri osa hindamine: Eesti juhtumiuuring), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Mahabubul Hasan, magistrikraad, 2021, (juh) Silvia Lips, Managing and Tracking e-Health Data Using Smart ID-Card in Bangladesh (E-tervise andmete haldus ja jälgimine Bangladeshi id-kaardi rakendamisel), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Helen Raamat, magistrikraad, 2021, (juh) Innar Liiv; Silvia Lips, Estonian Digital Public Service Improvement Analysis in Cross-Border Use Cases (Eesti avalike e-teenuste parendamise analüüs piiriüleste kasutusjuhtude jaoks), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Ruslan Kononov, magistrikraad, 2021, (juh) Sadok Ben Yahia; Silvia Lips, Evaluation of Facial Emotion Recognition Models for the Potential Deployment in Web-based Learning Environments (Näo emotsioonide tuvastamise mudelite võimalik rakendamine veebipõhistes õppekeskkondades), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut
- Natalia Vinogradova, magistrikraad, 2021, (juh) Silvia Lips, Re-Shaping the eIDAS Regulation from Stakeholders Perspective (eIDAS määruse muutmise perspektiivid sidusrühmade vaatenurgast), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

- Mohammed Saber Hafez Abdelhafis Sallam, magistrikraad, 2021, (juh) Silvia Lips, Success and Success Factors of the Estonian e-Residency from State and Entrepreneurs Perspective (Eesti e-residentsuse edutegurid riigi ja ettevõtjate vaatenurgast), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

- Oladele Solomon Amola, magistrikraad, 2021, (juh) Silvia Lips, Designing Crisis Management Mobile Application: a Case Study of Lagos State in Nigeria (Kriisiohjamise mobiilirakenduse kujundamine: Lagose osariigi juhtumiuuring Nigeerias), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

- Jose Ernesto Cueto Morales, magistrikraad, 2020, (juh) Silvia Lips, Improving the Digital Identity Management System in Mexico (Identiteedihalduse süsteemi parendamine Mehhikos), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

- Khayyam Zulfigarzada, magistrikraad, 2020, (juh) Silvia Lips, Designing Government e-Petition System in Azerbaijan (Aserbaidžaani avaliku sektori e-petitsiooni süsteemi disainimine), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

- Syed Mohsin Raza Naqvi, magistrikraad, 2020, (juh) Silvia Lips; Sidra Azmat Butt, Challenges and Opportunities of Applying e-ID (Smart National Identity Card) in Public Sector of Pakistan (Pakistani avalikus sektoris e-ID (riikliku ID-kaardi) rakendamise väljakutsed), Tallinna Tehnikaülikool, Infotehnoloogia teaduskond, Tarkvarateaduse instituut

9. Kaitstud lõputööd

- 2019, " Jätkusuutliku identiteedihalduse strateegia kavandamine kogemustega e-riigis", MSc, juhendaja Prof. Dirk Draheim, kaasjuhendaja dotsent Prof. Ingrid Pappel, Tallinna Tehnikaülikool, Tarkvarateaduste Instituut

- 2006, " Biomeetrilise tuvastamise andmekaitseõiguslikud aspektid", LL.M, juhendaja LL.M Rainer Osanik, kaasjuhendaja MA Veiko Kopamees, Tallinna Ülikool (endine Akadeemia Nord), Õigusteaduskond, era- ja äriõiguse õppetool

- 2004, "Eesti ja Inglismaa kindlustustegevuse õiguslik ning võrdlev analüüs", BSc, juhendaja LL.M Rainer Osanik, Tallinna Ülikool (endine Akadeemia Nord), Õigusteaduskond, era- ja äriõiguse õppetool

10. Teadustöö põhisuunad

- 4.6. Arvutiteadused

- 4.7. Info- ja kommunikatsioonitehnoloogia

11. Teadustegevus
Teadusartiklite, konverentsiteeside ja konverentsiettekannete loetelu on toodud ingliskeelse elulookirjelduse juures.

ISSN 2585-6901 (PDF)
ISBN 978-9916-80-021-8 (PDF)