Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership
Learning from the Case of Estonia

Lips, Silvia; Tsap, Valentyna; Bharosa, Nitesh; Krimmer, Robert; Tammet, Tanel; Draheim, Dirk

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

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] · Dirk Draheim[1]

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 & Dubey, 2019). Well-known examples of critical infrastructure are energy supply, transportation, food supply, water supply, healthcare (Filiol & Gallais, 2014), financial systems, civil administration, transportation systems, chemical industry (Alcaraz & 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

✉ Silvia Lips
   silvia.lips@taltech.ee

Extended author information available on the last page of the article.

---

[1] https://www.riigiteataja.ee/en/eli/525062018014/consolide

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 dirk 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 Section 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 Section 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 Section 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 Section 5, we provide a conclusion including an overview of research limitations and possible future research directions.

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 & Ayesiga, 2013; Ayo-Vaughan et al., 2019; Osei-Kyei & 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 & 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.

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 & 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 & 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 & Dubey, 2019). Ismail (2013) conducted a case study of Malaysia and identified five main success factors, i.e. "1) good governance; 2) commitment and responsibility of public and private sectors; 3) favourable legal framework; 4) sound economic policy; and 5) available financial market" (Ismail, 2013).

A lot of studies identify PPP success factors in developing countries (Ameyaw & Chan, 2016; Babatunde et al. 2016; Muhammad & 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 & 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 & Chan, 2016; Babatunde et al. 2016; Muhammad & 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

Table 1 Factors affecting PPP according to 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 Chan (2016)	PPP in water supply projects	"Commitment of partners, strength of consortium, asset quality and social support, political environment, and national PPP unit."

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".

[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/

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 & 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 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 Tables 2 and 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
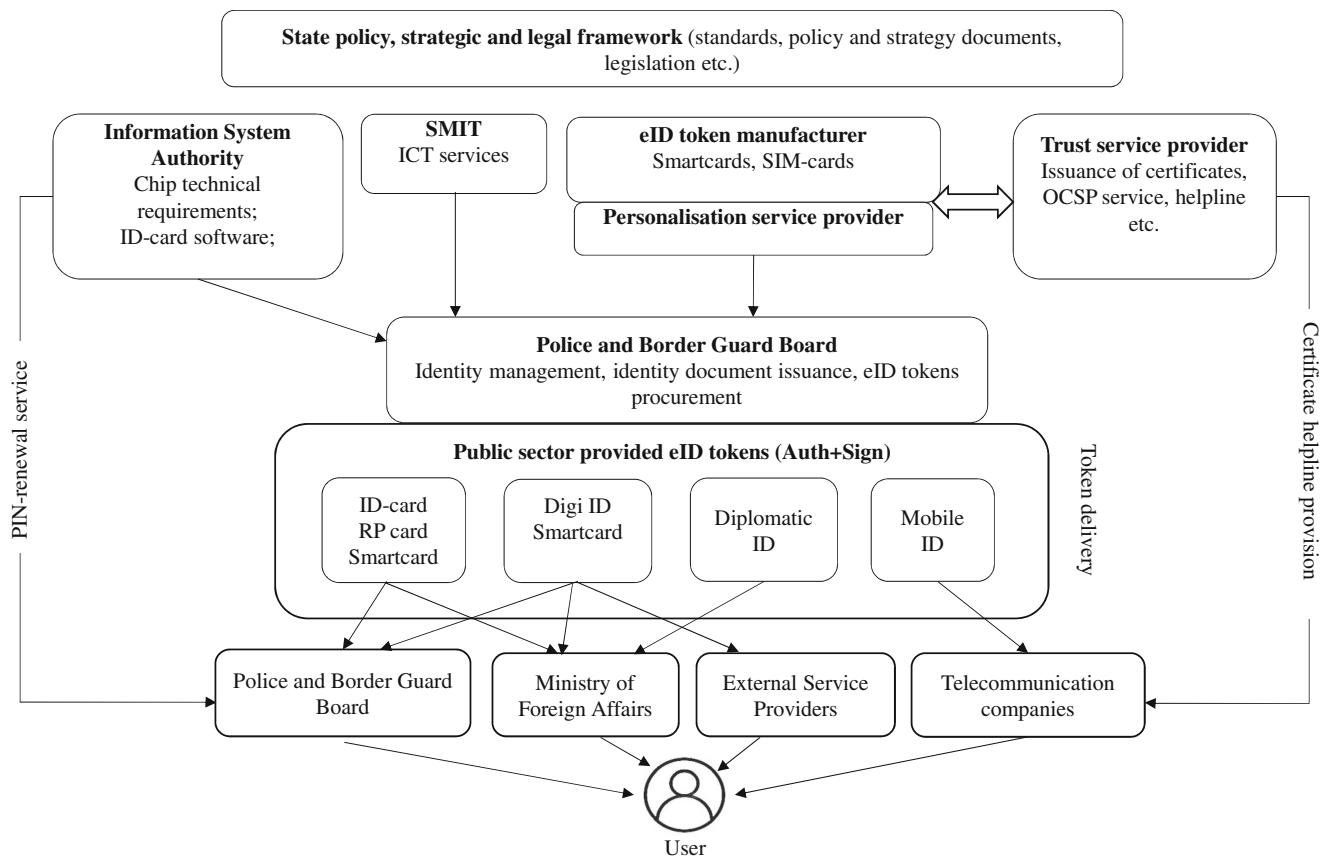
---

[7] https://blog.ria.ee/2018/05/

Fig. 1 The Estonian eID scheme from a stakeholders' perspective

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 & 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

---

[8] https://www.ria.ee/sites/default/files/content-editors/EID/valge-raamat-2018.pdf

Table 2 IMS (identity management system) stakeholders from the Estonian public sector and their roles

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.

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).

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;

    (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

Table 3 Estonian IMS private sector stakeholders 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 4 Estonian eID ecosystem analysis based on the model of (Koppenjan & Groenewegen, 2005)

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, Tables 2 and 3.

of the research results from their discussion. We present our findings according to 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

Table 5 Interview participants and their roles

| 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)/ Chair-man 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
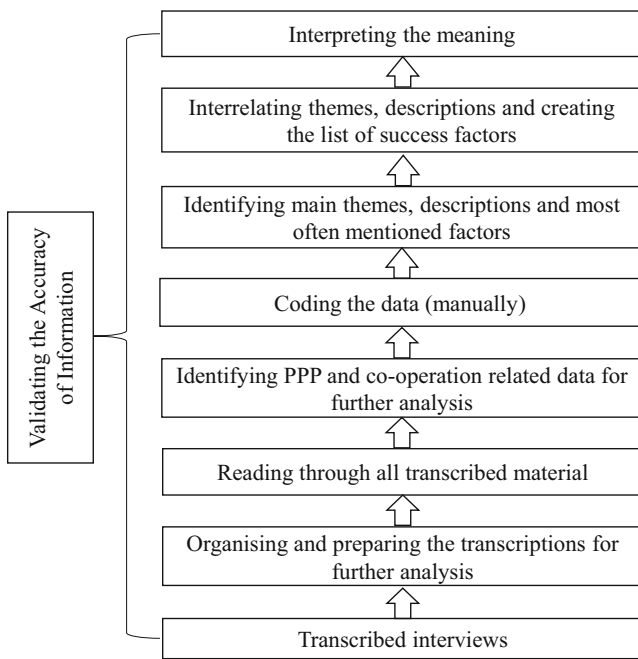
Fig. 2 Data analysis model

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 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.

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

Table 6 Positive versus negative aspects of the collaboration

Positive aspects	Negative aspects
• Joint meetings with a strategic focus	• Negative attitude and prejudices
• Workshops initiated by the public sector	• Poor involvement in discussions
• Public and private sector experts know each other from previous positions	• 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

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. 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
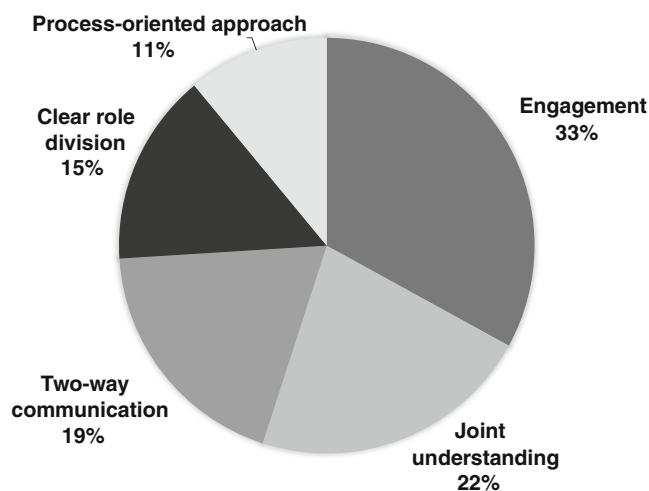
Fig. 3 Public-private cooperation success factors

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 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. As IT 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 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

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)

Proposals	Interviewees (anonymised)												Total
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	
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

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 Section 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

---

[12] https://cabforum.org/

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)

Cooperation Format	Interviewees (anonymised)												Total
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	
Moderated workshops	×	×				×	×			×	×		6
CA/Browser Forum format			×										1
Brainstorming									×				1
Visualization						×							1
Engagement of volunteers										×			1
Software development principles					×								1

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 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.

Declarations

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, E. E., & Chan, A. P. C. (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: Tallinn university of Technology Faculty of Systems Engineering, Department of Automation.

Ansper, A., Buldas, A., Freudenthal, M., et al. (2013). High-performance qualified digital signatures for X-Road. In H. R. Nielson, & D. Gollmann (Eds.) *Proceedings of NordSec 2013 – the 18th Nordic conference on secure it systems, lecture notes in computer science,* (vol.8208 pp. 123–138). Springer.

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, S. O., Opawole, A., & Akinsiku, O.E. (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, S. O., 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 S. Hofmann, C. Csáki, N. Edelmann, & 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 pp. 41–53). Springer International Publishing. https://doi.org/10.1007/978-3-030-58141-1_4.

Chan, A. P., Lam, P. T., Chan, D. W., 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, A. P. C., & 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, A. P. C., Lam, P. T. I., 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*, 4th edn. Thousand Oaks: SAGE Publications Inc., 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*, 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 L. Bellatreche, M. Dumas, P. Karras, et al. (Eds.) *Proceedings of ADBIS '2021 – the 25th European conference*

on advances in databases and information systems, (no.12843 pp. 7–12 in LNCS). Springer.

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* (pp. 47–57). West Lafayette.

Firmino, S. I. (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, P. A., & 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, D. T., Toan, N. Q., & 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, C. M., & Chang, L. M. (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, S. O. (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 K. Kastehein (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* (pp. 625–631). IEEE.

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* (pp. 45:1–45:8). ACM.

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 A. Kõ, & E. Francesconi (Eds.) *Proceedings of EGOVIS'2018 - the 7th international conference on electronic government and the information systems perspective, lecture notes in computer science,* (vol. 11032 pp. 60–70). Cham:Springer. 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 A. Kõ, E. Francesconi, G. Anderst-Kotsis, & 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 pp. 221–234). Berlin:Springer. 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* (pp. 31–37). IEEE. 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, A. P. C. (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, A. P. C. (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. (2018). On the systematic exploitation of the Estonian data exchange layer X-Road for strengthening public private partnerships. In A. Kankanhalli, A. Ojo, & D. Soares (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. (2018). 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* (pp. 34–41). ACM.

Petersson, A. M., & 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, A. O. (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* (pp. 216–222). IEEE.

Schuppert, G. F. (2015). Governance. In J. D. Wright (Ed.) *International encyclopedia of the social & behavioral sciences* (4th ed., pp. 292–300). Oxford:Elsevier. hhttps://doi.org/10.1016/B978-0-08-097086-8.75020-3.

Sehgal, R., & Dubey, A. M. (2019). Identification of critical success factors for public–private partnership projects. *Journal of Public Affairs*, *19*(4), e1956.

Sein, M. K., Henfridsson, O., Purao, S., et al. (2011). Action design research. *MIS Quarterly*, *35*(1), 37–56. https://doi.org/10.2307/23043488.

Surachman, E. N., 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, E.W.L. (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. (2020). Analyzing eID public acceptance and user preferences for current authentication options in Estonia. In A. Kö, E. Francesconi, G. Kotsis, & 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 pp. 159–173). Cham: Springer. https://doi.org/10.1007/978-3-030-58957-8_12.

Tsap, V., Lips, S., & Draheim, D. (2020). eID public acceptance in Estonia: towards understanding the citizen. In S. J. Eom, & J. Lee (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*. New York: United Nations.

UN Department of Economic and Social Affairs. (2020). *E-government survey – digital government in the decade of action for sustainable development*. New York: United Nations.

Vaismoradi, M., Turunen, H., & 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 A. Kö, E. Francesconi, G. Kotsis, 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 pp. 73–85). Cham: Springer.

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 3rd international conference on availability reliability and security 2008* (pp. 572–577).

Williamson, O. E. (1979). Transaction cost economics: the governance of contractual relations. *The Journal of Law & Economics*, *22*(2), 233–261.

Williamson, O. E. (1998). Transaction cost economics: how it works; where it is headed. *The 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, R. K. (2011). *Applications of case study research*. Los Angeles: Sage.

Zhang, X. (2005). Critical success factors for public–private partnerships in infrastructure development, *Journal of Construction Engineering and Management*, https://doi.org/10.1061/(ASCE)0733-9364(2005)131:1(3).

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 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 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 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 is a full professor of applied artificial intelligence at Tallinn University of Technology. His main research interests include crowd-sourced 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 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".

Affiliations

Silvia Lips[1] · Valentyna Tsap[2] · Nitesh Bharosa[3] · Robert Krimmer[4] · Tanel Tammet[5] · Dirk Draheim[1] (iD)

✉ Dirk Draheim
dirk.draheim@taltech.ee

Valentyna Tsap
valentyna.tsap@cyber.ee

Nitesh Bharosa
n.bharosa@tudelft.nl

Robert Krimmer
robert.krimmer@ut.ee

Tanel Tammet
tanel.tammet@taltech.ee

[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