DIGITAL PUBLIC SERVICE IMPROVEMENT IN CROSS-BORDER USE CASES

HELEN RAAMAT,[1] INNAR LIIV,[2] SILVIA LIPS,[3]
ROZHA KAMAL AHMED,[4,5] RAHUL SHARMA,[4,6]
DIRK DRAHEIM[4]

[1] Information System Authority, Tallinn, Estonia
helen.raamat@ria.ee
[2] Tallinn University of Technology, Tallinn, Estonia
innar.liiv@taltech.ee
[3] Information System Authority, Tallinn, Estonia
silvia.lips@taltech.ee
[4] Tallinn University of Technology, Information Systems Group, Tallinn, Estonia
rozha.ahmed@taltech.ee, rahul.sharma@taltech.ee, dirk.draheim@taltech.ee
[5] Sulaimani Polytechnic University, Computer Science Institute, Sulaymaniyah, Iraq
rozha.ahmed@spu.edu.iq
[6] Ajay Kumar Garg Engineering College, Ghaziabad, India
rahul.sharma@taltech.ee

This research identifies the main legal and technical barriers connected to identity management and cross-border service provision. We also propose a solution that fits in the current state of play. We analyzed the existing documentation and conducted semi-structured interviews with digital public service providers and use the Estonia as a case study to map the current obstacles. To resolve the cross-border interoperability issues that digital public services face, we explore the existing state of play for cross-border use cases through a process design and highlighting the requirements for cross-border interoperability infrastructure. As a result, we provide recommendations overcoming the barriers that affect cross-border digital public service delivery.

Keywords:
interoperability, cross-border digital public services, eIDAS, SDGR, implementation challenges, electronic identity

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.4.2024.15
ISBN 978-961-286-871-0

1 Introduction

The mobility of European Union (EU) citizens has grown in recent years, as well as the demand and expectations to access cross-border digital public services (European Commission, 2021). The regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) was established on July 23rd, 2014, in the EU to support the objectives of the digital single market and digital economy.[1] eIDAS aims to facilitate access to cross-border digital services by creating trust in the digital world, like in the physical world. According to the regulation, all the public and private sector authorities providing digital public services in the EU must mutually recognize the notified eID means. For the implementation of eIDAS, the European Commission's (EC) Connecting Europe Facility (CEF) has created an eID building block that provides a framework and a software platform for cross-border interoperability – eIDAS-Node.[2] As of 2020, most EU member states have already implemented eIDAS-Node in their national eID infrastructure. Although the eIDAS-Node software platform enables functionality for cross-border identification in EU digital public services, the accessibility to cross-border digital services under the eIDAS framework remains low. The implementation of the Single Digital Gateway Regulation (SDGR)[3] foresees the increased use of electronic identification (eID) transactions across the EU (Kalvet et al., 2018). Therefore, it is necessary to specify what the cross-border eID infrastructure must provide to meet the needs and expectations of the Single Digital Gateway initiatives.

During the research, we identify the main legal and technical barriers connected to identity management and service provision that prevent the cross-border use of digital public service procedures and provide a solution for changes that can fit in the current state of play. We aim to answer the following research questions:

RQ 1. What are the key barriers that prevent seamless digital service delivery of (Estonian) public services in cross-border use cases by the means of EU member state notified eID?

[1] eIDAS regulation. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[2] eIDAS-Node integration package. Available: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS-Node+Integration+Package
[3] SDGR regulation. Available: https://eur-lex.europa.eu/eli/reg/2018/1724/oj

SRQ 1.1 How do the barriers affect the seamless delivery of (Estonian) digital public services in cross-border use cases on the legal, organizational, technical, and operational levels?

RQ 2. How should the cross-border infrastructure be improved for seamless digital public service delivery?

SRQ 2.1. What are the key requirements for successfully implementing a fully digital cross-border public service?

The research is based on an Estonian case study. However, the outcomes of this study could be adopted as an example by other countries with similar e-government infrastructure. More specifically, we focus on a cross-border scenario where an alien with an eID from one of the EU Member States wants to access one of the Estonian digital public service procedures. To map the current existing obstacles and a state of play, we rely on document analysis and semi-structured interviews conducted with digital public service providers in Estonia. As a result, we provide recommendations on how the barriers that affect cross-border digital public service delivery in Estonia could be overcome.

This paper is organized as follows. In Sect. 2, we provide an overview of the EU's current interoperability framework. In Sect. 3, we present our research design and methodology. Sect. 4 gives an overview of the main research findings. In Sect. 5, we propose a solution for identity matching and make recommendations. Finally, we conclude the paper in Sect. 6 with the future research perspective.

2 Interoperability in the European Union

In the need for specific common guidance on creating interoperable and high-quality digital public services, on 23 March 2017, the European Commission adopted the European Interoperability Framework (EIF) (Kalogirou & Charalabidis, 2019). The framework covers 12 underlying principles of European public services: subsidiarity and proportionality (1), openness (2), transparency (3), reusability (4), technological neutrality and data portability (5), user-centricity (6), inclusion and accessibility (7), security and privacy (8), multilingualism (9), administrative simplification (10),

preservation of information (11), assessment of effectiveness and efficiency (12) (European Commission, 2017). The EIF presents an interoperability model, where the interoperability is classified into four layers, containing legal, organizational, semantic, and technical interoperability (European Commission, 2017).

The goal of adopting the eIDAS on the 23rd of July 2014 was to provide an EU-wide legal framework that enables secure and seamless electronic interactions between businesses, citizens, and public authorities (Lips et al., 2020). To support the interoperability of eIDs, the European Commission (EC) created the eID and eSignature building blocks to help member states' public administrations and digital service providers extend the existing infrastructure for a secure cross-border service delivery.[4]

The eIDAS regulation supports the secure mutual recognition of cross-border eIDs, which is backed with a respective framework and a technical system of eIDAS-Node. [5] The goal of the eIDAS-Node solution is to provide all Member States with an EU-compliant reference platform that enables interoperability between different eID protocols and standards. To establish cross-border recognition using eIDAS-Node software, the Member State must configure the software in its national infrastructure and implement an interface between the national eID ecosystem and the eIDAS network.

eIDAS-Node supports two main cross-border scenarios: requesting and providing cross-border authentication. Figure 1 explains how the interoperability in the eIDAS Network is approached using the eIDAS-Nodes. The eIDAS-Node consists of three components:

- eIDAS-Proxy-Service: a component that provides authentication data.
- eIDAS-Connector: a component that requests cross-border authentication.
- eIDAS-Middleware-Service: a component that provides authentication data and is being provided by the sending Member State and operated by a receiving member State.[6]

[4] https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/
[5] https://digital-strategy.ec.europa.eu/en/policies/electronic-identification
[6]https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS-Node+version+2.0

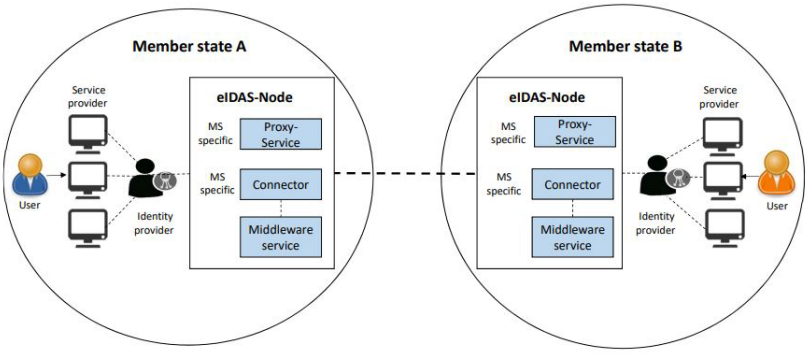

Figure 1: The overview of the interoperability components in eIDAS Network
Source: https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Proxy+to+proxy

Estonia has implemented the eIDAS-compliant authentication gateway service (also known as TARA).[7,8] Estonian eID ecosystem is described in detail in various other research papers (Lips et al., 2019; Saputro et al., 2020; Lips et al., 2023). The SDGR Article 14 sets requirements to establish a technical system for the cross-border automated data and evidence exchange between competent authorities in different member states and the application of the Once-Only Principle (OOP) for the online procedures. The Once Only Technical System is an EU-wide technical system currently under development, supervised, and provided by the European Commission. The OOP system aims to eliminate the administrative burden for citizens, public services, and businesses in the EU. It allows the sharing and reuse of data in real-time across borders, facilitating access to public cross-border online procedures and providing an automated exchange of evidence (Tepandi et al., 2021).

[7] https://github.com/e-gov/eIDAS-SpecificProxyService
[8] https://e-gov.github.io/TARA-Doku/TechnicalSpecification

3 Research Design and Methodology

The research follows the case study research methodology (Yin, 2018). We used multiple data sources during the research, including documents, archival records, and qualitative interviews (Creswell, 2016).

We used descriptive case study methodology to understand the impact of the requirements on the implementation of cross-border digital services in compliance with SDGR and strengthen the existing theoretical knowledge. During the research, we mapped the current state of play of the cross-border service provision in Estonia and provided an improved process design based on the SDGR online procedures. To improve the validity of the outcomes in this study, we analyze the two observed cases using the cross-case synthesis method.

The ideas for the proposed solution were based on the input from the qualitative data analysis, as well as on the practical experience in the field of cross-border services and electronic identification. The research results were validated through the process design and official documentation.

During the research, we conducted semi-structured interviews with the key stakeholders of the online electronic procedures specified in Annex II of the SDGR. We contacted 24 experts from 14 Estonian public sector bodies via e-mail and phone. In total, 14 interviewees responded with an interest in contributing. A list of the interviewees is provided in Table 1. The interview participants were selected based on the SDGR Annex II procedures and their relation to the service providers at the national level.

During the data collection phase, six expert interviews were conducted with various experts: four individual and two group interviews. The group interview form was chosen due to the data's richness and high quality (Flick, 2022). Although group interviews are typically structured in their form, we chose to keep the semi-structured format throughout all the interviews as most of them were conducted in a semi-structured form. The interviews were conducted in Estonian and recorded using voice recording applications, Voice Memos by Apple, and Skype call recording tool for transcript writing and further analysis.

Table 1: List of interviewees

Government body	Interviewee	Duration
Ministry of the Interior	2 experts from the Population Facts Department	53:43
Estonian Social Insurance Board	1 expert from the Benefits Department	49:56
Estonian Road Administration	7 experts from the E-services and Information Technology Department	55:11
Health and Welfare Information Systems Centre	Systems architect	51:29
Estonian Tax and Customs Board	1 expert from the Tax Department	38:05
Estonian Tax and Customs Board	2 experts from the Public Services Department	31:26

The data analysis in this research relies on three qualitative analysis techniques that were used to identify patterns, themes, and sequences of the data that had been previously collected. Documenting at each step in the research analysis allows trustworthy and valid conclusions to be achieved that explain the chain of evidence to the readers (Runeson et al., 2012). We use document analysis and thematic analysis following the guidelines provided by Braun and Clarke (Braun & Clarke, 2006). We also use triangulation of multiple data sources to strengthen the validity of the research results (Salkind, 2010).

As a result, we propose a solution for improving the existing cross-border service provision process based on the theoretical framework and existing processes. We use the UML diagrams to interpret, assess, and validate the research results.

4 Research Findings

During the thematic analysis, based on the qualitative interviews, we identified four following themes: accessibility (A), data exchange (DE), identity management (IM), and interoperability (IO). These themes highlight the key findings of the current state of cross-border service provision based on the SDGR services in Estonia, the main obstacles, and the requirements for a successful cross-border service delivery. Figure 2 gives a detailed overview of the themes and codes.

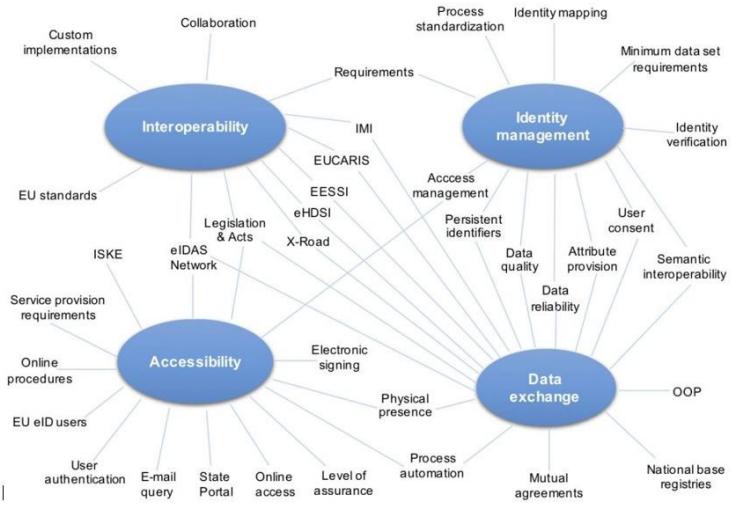

Figure 2: Overview of the themes and codes

Table 2: Key requirements for cross-border digital service provision

ID	Requirement	Description	Theme
R-1	**Existing Estonian PIC[9]**	One of the most highlighted requirements by the current service provision concept is having the Estonian PIC. Without the latter, only a few digital public services are available for EU eID users. The data of the authenticated users is requested from and verified against the base registries, such as the Estonian population register, using the X-Road data exchange platform. It was also pointed out by more than half of the interviewees that currently, there are not many SDGR Annex II online procedures available in Estonia for EU eID users who do not have an existing event in the population register nor have issued an Estonian PIC.	A, IO
R-2	**Existing events in the base registries for identity verification**	All the interviewees highlighted that one of the first and primary sources for the current identity mapping procedures relies on the data requested from the Estonian population register.	A, DE, IM, IO

[9] Personal Identification Code

ID	Requirement	Description	Theme
R-3	**Unified cross-border platform for automated cross-border data exchange**	Since the X-Road, which already permits the automated exchange of evidence, has been widely adopted in e-Estonia, Estonian digital service providers would prefer using this platform for automated cross-border data exchange between EU countries. Problem: The key requirement here is that there must be an existing record in the population register to perform a secure identity mapping procedure. Since no standardized identity mapping procedure is currently in use for the base registries, the data exchange of a new incoming EU eID user's attributes is blocked over the X-Road, which directs us back to the accessibility issue.	DE, IO
R-4	**Persistent PIC across EU**	The main cross-border automated data exchange obstacle mentioned throughout the interviews was that many countries do not provide a joint identifier for natural persons, similar to Estonia. For example, each government authority assigns different identifiers to their citizens in Germany. That, in turn, brings along the mapping procedure. If the latter could be automatized, the cross-border data exchange could significantly raise the data quality.	DE, IM, IO
R-5	**Automatized identity mapping procedure**	Since identity mapping highly relies on the existing records of a person in the base registries, the online verification of EU eID users can only be reliably performed with cross-border automated data exchange. According to the interviewees, the central issue they hope to resolve in the future is automating the identity mapping procedures.	IM
R-6	**Standardized identity mapping procedure**	All the interviewees highlighted that one of the first and primary sources for the current identity mapping procedures relies on the data requested from the Estonian population register. It was pointed out that to automatize the process, there should be internationally agreed standards for semantically describing the identities across registries. Therefore, semantic interoperability could bring identity mapping to the next level.	IM
R-7	**Sufficient provision of attributes for identity mapping**	The efficient and reliable identity mapping should highly rely on the additional attributes that are sufficient and persistent as possible in time, including PIC, first name(s), family name(s), date of birth, country (as a prefix), current address, gender, nationality, place of birth.	IM
R-8	**Semantically interoperable attributes**	Semantically interoperable attributes are one of the key enablers for seamless data exchange and data management.	IM

Based on the interview results, we created a list of high-level requirements for cross-border digital service provision. Table 2 summarizes the key requirements and related themes based on the case of Estonia.

The documentation and thematic analysis identified a common issue of the current cross-border service provision concept across all the life events of the SDGR analysed in this research – a lack of common understanding and non-existent standards for identity management. Moreover, we identified the following barriers and factors that affect the cross-border interoperability of public services:

1) The complexity of the eID notification process slows down the recognition and, thereby, the accessibility to digital services and procedures for EU citizens.
2) The lack of unique and persistent identifiers on the access to digital services.
3) Due to the limitations in national policies and law in many EU countries, the cross-border exchange of data and evidence a citizen can be limited, which affects the overall success of the EU-wide adoption of the eIDAS and OOP in SDGR.
4) The lack of clear and standardized interoperability profile and reliable identity attributes in the EU on how to semantically describe the identities across registries.
5) Missing standardized and automatized approach on identity matching at the EU and national level. Since identity matching relies on the existing records of a person in the base registries, the verification of EU eID users cannot be reliably performed without cross-border automated data exchange.
6) Different levels of assurance of eID means in the EU affect the availability of cross-border services.
7) The e-government systems and national service providers cannot handle the format of foreign identifiers. Therefore, the national identifier (PIC in Estonia) is a prerequisite for access to public services.

5 Proposed Solution for Identity Matching and Recommendations

Based on the key requirements presented in Table 2 and analysing two Estonian cross-border evidence exchange cases, requesting proof of residence and requesting proof of registration of birth, we propose a solution for identity matching presented in Figure 3.

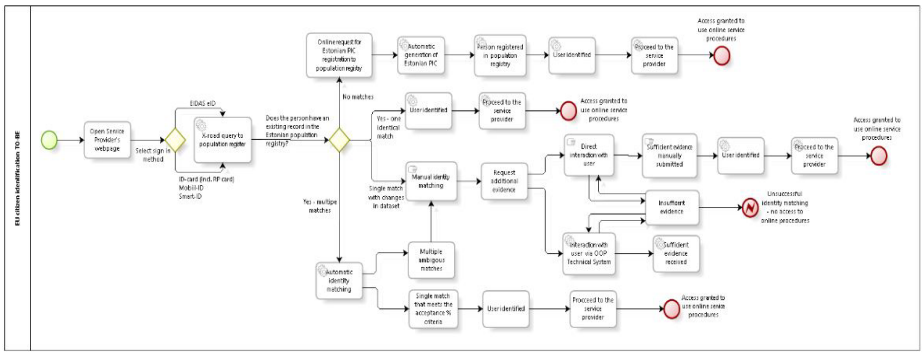

Figure 3: Proposed solution for authentication of EU citizens
Source: Own

The cross-border availability of attributes highly affects the reliability of identity-matching mechanisms. In the UML scheme, an assumption is made that when a matching identity has been found, an existing Estonian PIC is already assigned to the EU citizen. The centralized approach to an identity-matching system is recommended to reduce the burden for the service providers and increase the quality and reliability of the identity-matching system. Assigning a national identifier, such as Estonian PIC, to the eIDAS eID users helps provide a seamless user experience and enables automatic enrolment.

In order to request additional evidence and attributes from authoritative sources in cross-border use case scenarios, the OOP technical system and eIDAS-Node could facilitate access to cross-border data. As the eIDAS regulation is currently under revision, we make the following suggestions:

1) The expansion of the mandatory eIDAS minimum data set attributes to improve reliable matching of identities. Ideally, the mandatory data set should consist of the attributes that are sufficient and persistent as possible in time, including PIC, first name(s), family name(s), date of birth, country (as a prefix), current address, gender, nationality, place of birth.
2) The eIDAS eID notification procedure should emphasize the importance of unique identity attributes for cross-border use and, where possible, the unique identifier should ideally be the same for digital and physical eID to improve reliability.
3) All EU countries should consider notifying at least one eID scheme that meets the highest level of assurance to improve the accessibility and availability of cross-border public services.

Reusing the attribute information from base registries is essential for efficient and user-centric cross-border service delivery. Technical, legal, and semantical aspects must support the exchange of cross-border attributes.

The centralized approach to the identity matching system is recommended to reduce the burden for the service providers and increase the quality and reliability of the identity matching system. As presented in the cross-case synthesis, the Estonian PIC can be used as a workaround for enabling access to foreign eID to Estonian public services and online procedures. Assigning a national identifier, such as Estonian PIC, to the eIDAS eID users helps provide a seamless user experience and enables automatic enrolment. However, some limitations apply to issuing Estonian PIC to foreign identities. The specific structure of Estonian PIC includes information about a person that cannot always be provided with the current minimum data set of eIDAS eID, such as gender. However, it can be retrieved if the eID country provides the additional attributes.

1

6 Limitations and Future Work

The main legal and organizational barriers identified in this study refer to the limitations in national policies and law in many EU countries, where the cross-border exchange of identity attributes remains limited or low. This affects the overall success of the EU-wide adoption of the eIDAS and OOP in SDGR. As a result of the research, we propose a possible solution for identity matching based on the Estonian example and further recommendations. However, it is essential to continue the research and develop the proposed identity matching framework further, especially in the context of eIDAS 2.0, which will be adopted and implemented very soon.[10] It is also possible to continue the research at the more theoretical level.

Since the SDGR implementing regulation has yet to be adopted and the OOP technical system has yet to be released, the author sees a further need to analyse the cross-border service provision improvement in Estonia. In recent years, the demand for cross-border services has increased in the EU and outside the EU borders. Therefore, the analysis of the EU interoperability frameworks, such as

[10] eIDAS 2.0. Available:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0281

eIDAS and SDGR, could be extended and analysed in the context of third countries.

7 Conclusion

This research has identified that cross-border digital service accessibility highly relies on the following factors: 1) secure identification, 2) cross-border functional and secure attribute exchange, 3) automatized identity matching based on sufficient attributes, and 4) cross-border evidence exchange for specific procedures based on the OOP technical system.

To sum up, we visualized the research findings and answers to the research questions in Figure 4.

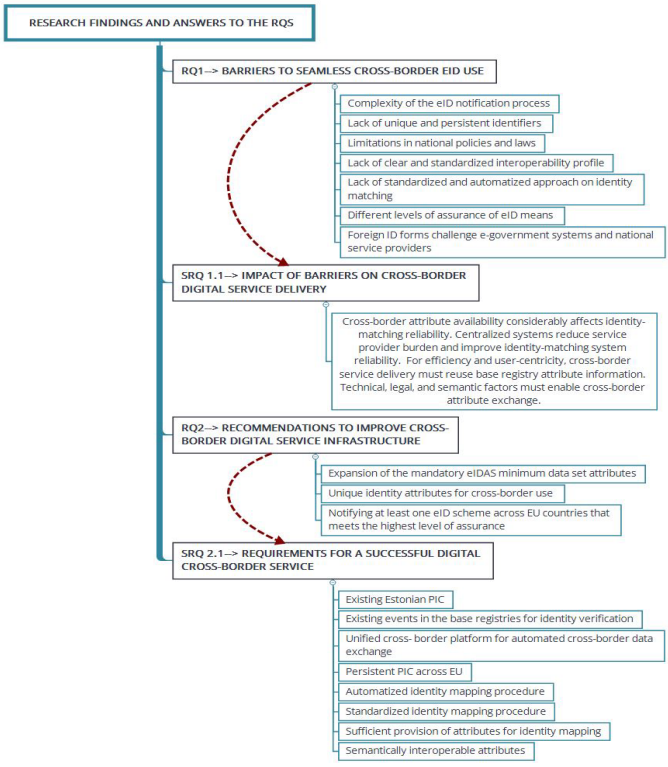

Figure 4: Summary of the research findings and answers to the research questions
Source: Own

References

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

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

European Commission. Directorate General for Informatics. (2017). New European interoperability framework: promoting seamless services and data flows for European public administrations. Publications Office. https://doi.org/10.2799/78681

European Commission. (2021). 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0124

Flick, U. (2022). An introduction to qualitative research. An introduction to qualitative research, 1-100.

Kalogirou, V., & Charalabidis, Y. (2019). The European union landscape on interoperability standardisation: status of European and national interoperability frameworks. In Enterprise Interoperability VIII: Smart Services and Business Impact of Enterprise Interoperability (pp. 359-368). Springer International Publishing.

Kalvet, T., Toots, M., van Veenstra, A. F., & Krimmer, R. (2018, April). Cross-border e-government services in Europe: expected benefits, barriers and drivers of the once-only principle. In Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance (pp. 69-72).

Lips, S., Aas, K., Pappel, I., & Draheim, D. (2019). Designing an Effective Long-Term Identity Management Strategy for a Mature e-State. In Electronic Government and the Information Systems Perspective (pp. 221–234). Springer International Publishing. https://doi.org/10.1007/978-3-030-27523-5_16

Lips, S., Bharosa, N., & Draheim, D. (2020, November). eIDAS implementation challenges: the case of Estonia and the Netherlands. In International conference on electronic governance and open society: challenges in Eurasia (pp. 75-89). Cham: Springer International Publishing.

Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T., & Draheim, D. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. Information Systems Frontiers, 1-18.

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

Salkind, N. J. (Ed.). (2010). Encyclopedia of research design (Vol. 1). sage.

Saputro, R., Pappel, I., Vainsalu, H., Lips, S., & Draheim, D. (2020, April). Prerequisites for the adoption of the X-Road interoperability and data exchange framework: a comparative study. In 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 216-222). IEEE.

Tepandi, J., Rotuna, C., Sellitto, G. P., Fieten, S., & Prentza, A. (2021). The Technical Challenges in OOP Application Across the European Union and the TOOP OOP Architecture. In The Once-Only Principle: The TOOP Project (pp. 141-163). Cham: Springer International Publishing.

Yin, R. K. (2018). Case study research and Applications Design and methods.