

**eIDAS Implementation Challenges
The Case of Estonia and the Netherlands**

Lips, Silvia; Bharosa, Nitesh; Draheim, Dirk

DOI

[10.1007/978-3-030-67238-6_6](https://doi.org/10.1007/978-3-030-67238-6_6)

Publication date

2020

Document Version

Final published version

Published in

Electronic Governance and Open Society

Citation (APA)

Lips, S., Bharosa, N., & Draheim, D. (2020). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In A. Chugunov, I. Khodachek, Y. Misnikov, & D. Trutnev (Eds.), *Electronic Governance and Open Society: Challenges in Eurasia - 7th International Conference, EGOSE 2020, Proceedings* (pp. 75-89). (Communications in Computer and Information Science; Vol. 1349). Springer.
https://doi.org/10.1007/978-3-030-67238-6_6

Important note

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

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Green Open Access added to TU Delft Institutional Repository




'You share, we take care!' - Taverne project

<https://www.openaccess.nl/en/you-share-we-take-care>

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.



eIDAS Implementation Challenges: The Case of Estonia and the Netherlands

Silvia Lips¹ , Nitesh Bharosa² , and Dirk Draheim¹ 

¹ Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia
{Silvia.lips, dirk.draheim}@taltech.ee

² Delft University of Technology, Postbus5, 2600 AA Delft, The Netherlands
n.bharosa@tudelft.nl

Abstract. Solid eID (electronic identification) infrastructures form the backbone of today's digital transformation. In June 2014, the European Commission adopted the eIDAS regulation (electronic identification and trust services for electronic transactions in the internal market) as a major initiative towards EU-wide eID interoperability; which receives massive attention in all EU member states in recent years. As a joint effort of Estonia and the Netherlands, this study provides a comparative case study on eIDAS implementation practices of the two countries. The aim was to analyze eIDAS implementation challenges of the two countries and to propose a variety of possible solutions to overcome them. During an action learning workshop in November 2019, key experts from Estonia and the Netherlands identified eIDAS implementation challenges and proposed possible solutions to the problems from the policy maker, the service provider and the user perspective. As a result, we identified five themes of common challenges: compliance issues, interpretation problems, different practices in member states, cooperation and collaboration barriers, and representation of legal persons. Proposed solutions do not only involve changes in the eIDAS regulation, but different actions to develop an eIDAS framework and to improve cross-border service provision - which has recently become an important topic among member states. Eventually, the study provides practical input to the ongoing eIDAS review process and can help member states to overcome eIDAS implementation challenges.

Keywords: eIDAS · Electronic authentication · Electronic identity · Implementation challenges · Identity management

1 Introduction

Digital transformation of countries offers many opportunities, but at the same time reduces control over their operating environment [1]. More and more, public and private sector organisations offer their services online and across borders. To access these e-services, implementation of an accurate and reliable digital authentication procedure together with a digital signature option is essential [2, 3].

In July 2014, the European Commission (EC) adopted regulation No 910/2014 [4] on electronic identification and trust services for electronic transactions in the internal market (eIDAS) to enable a secure and seamless electronic data exchange and interaction of public and private entities and users, not only inside the member states, but also across the European Union (EU). This initiative is part of the EU Digital Single Market strategy [5] and mandatory for all EU member states since September 2018 [4].

The implementation of the eIDAS regulation and its first years of implementation have raised many practical questions and revealed various research gaps. According to the eIDAS regulation Article 49, the EC shall review the regulation by 01.07.2020 latest to evaluate whether the regulation needs to be modified [4]. The EC has already initiated a feedback collection process among its member states. In parallel with the ongoing eIDAS implementation actions, EC progressed further and adopted in October 2018 SDGR regulation, which established a single digital gateway to provide access to information, procedures and for assistance and problem-solving services, also known as the SDGR regulation [6]. The aim of this regulation is to simplify access to cross-border administrative services for citizens and companies [7]. One pre-condition for the SDGR implementation is successful and smooth eIDAS implementation in the member states. Therefore, it is now the perfect time to analyze the implementation practices of different EU countries and to provide relevant feedback to the ongoing evaluation process.

We decided to research the practices of Estonia and the Netherlands. Both of the countries have stable and functional e-government, but at the same time, they have different e-governance models and approaches to the eIDAS implementation [8].

The aim of this research paper is to analyze eIDAS implementation challenges of Estonia and the Netherlands and to propose a variety of possible solutions to overcome them. The research objectives are therefore to:

- 1) Identify the challenges Estonia and the Netherlands faced during the implementation of eIDAS from the user's, the service provider's and the policy maker's perspective; and
- 2) Recommend possible solutions to overcoming identified challenges.

We use a comparative case study research approach [9] together with action learning methodology [10] to analyse above-mentioned research questions.

The paper is organized as follows. Section 2 provides background information about the current eIDAS implementation situation in Estonia and the Netherlands and an overview of important related literature. Section 3 presents the research design and gives insight into the used theoretical framework. Section 4 sums up research findings from the policy maker, service provider and user perspective. In Sect. 5, we discuss the research results and make recommendations to the eIDAS review process. Section 6 provides an insight to the future research perspective followed by Sect. 7 that concludes the study.

2 Background

In this section, we provide a brief overview of existing literature on eIDAS implementation. In addition, to understand the results of this paper, it is important to introduce shortly the eIDAS implementation state and situation in Estonia and the Netherlands.

2.1 eIDAS Implementation in the EU from the Literature Perspective

The eIDAS regulation has been in force for more than five years, of which it has been actively implemented and used over the past two years. According to the regulation itself, voluntary recognition of electronic identities were possible since September 2015, rules for trust service providers had to be adopted by July 2016 and cross-border recognition of electronic identities was enabled by September 2018 [5]. First countries notified their eID schemes¹ under eIDAS already in 2017 (Germany) and 2018 (Estonia, Spain, Croatia, Belgium etc.). The implementation process itself is complex and time-consuming. Figure 1 illustrates the steps that member states have to pass to notify their eID schemes.



Fig. 1. eID scheme notification process.

From a research perspective, the topic is quite new; and, so far, it has been handled rather from the angle of a specific country or sector. For example, several studies focus on the academic sector, e.g., on how to build eIDAS-based cross-border services in the education and to enable secure and seamless interaction between different parties [11–15]. The focus is mainly on solving the practical problems: how to transport new data attributes through eIDAS infrastructure solutions [11, 13], how to implement eIDAS-based academic services and create secure connections between academic services and the national eIDAS node [12, 13]. Some studies are even more specific and concentrate on a part of an eIDAS node that member states have to modify independently [14].

Several studies focus on eIDAS implementation challenges in a particular country [16–18]. In case of United Kingdom (UK), it is questionable if the country should notify their eID scheme and does the existing system complies with the eIDAS privacy and data protection requirements [17]. Pelikánová, Cvik and MacGregor analyze and

¹ According to eIDAS, an eID scheme is a system for electronic identification under which electronic identification means are issued to natural or legal persons (or to natural persons representing legal persons).

evaluate the eIDAS adoption in the Czech public sector bodies and compare the results with some other EU member states practice. Their research results show a lot of hesitation and passivity in the Czech public sector while adopting eIDAS requirements [18].

Other research projects focus more on different aspects of the regulation, such as security, privacy [19, 20] and data protection issues [21]. From the data protection perspective, Tsakalakis, Stalla-Bourdillon and O’Hara argue that technical architecture of an eID scheme affects the level of data protection. They propose that the use of pseudonyms and selective disclosure help to fulfill the data minimization and purpose limitation principles [21]. Only few studies analyze different identification and trust services compatible with the eIDAS regulation in wider context and do not focus on a particular member state [22].

While conducting the literature overview it became clear that many of the studies focus on specific sectors or solve very concrete data exchange or integration issues in the eIDAS context. We did not find pan-European studies addressing eIDAS implementation practices in various member states with proposals to improve the current environment. Therefore, our research aims to fill this significant research gap and to provide recommendations for the further eIDAS review process.

2.2 Estonia

Estonia has implemented eIDAS according to the EC timetable and notified its eID scheme on assurance level “high” in November 2018. The notification consisted of six different eID tokens: ID-card, residence permit card, digital identity card, e-residency digital identity card, mobile-ID and diplomatic identity card.²

The Estonian eID management is based on tight public-private cooperation. Public sector authorities are responsible for personal identification, identity management, eID infrastructure management and supervisory activities. Private sector organization offers eID tokens as well as personalization and trust services [23]. In December 2018, Estonia changed the eID token manufacturer and since then, has issued the fourth generation electronic of identity cards [24].

All previously mentioned electronic identities are in active use and the public acceptance of the eID is high [25, 26]. According to the latest statistics from March 2020, there are more than 1,35 million eID cards and around 234 000 mobile-ID’s issued by the public sector. In February 2020, the total amount of transactions related to eID’s exceeded 37 million.³

² Estonian eID scheme notified under eIDAS, <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia>.

³ Estonian eID statistics, <https://www.id.ee/?lang=en&id=>.

In addition to the public sector eID tokens, the local trust service provider SK ID Solutions AS issues QSCD (Qualified Signature Creation Device) certified Smart-ID for authentication and signing purposes.⁴ More than 500 000 users also actively use this solution.⁵

2.3 The Netherlands

In 2019, the Netherlands notified its electronic identification trust framework for businesses, also known as eHerkenning, on the assurance levels “substantial” and “high”.⁶ There are several authentication service providers in the country (i.e., Connectis, Digidentity, KPN, QuoVadis, Reconi, and Unified Post).⁷

In December 2019, the Netherlands pre-notified another authentication service named “DigiD. This solution enables authentication of natural persons in relation with the governmental authorities and organizations that perform public tasks. Logius, an organization operating in the governing area of the Dutch Ministry of the Interior and Kingdom Relations, manages and maintains the DigiD in the Netherlands [27].

Around 80% (14 million people) of the Dutch population use the service. More than 650 service providers are connected to the DigiD service. According to the statistics, DigiD service processes over 300 million authentication requests per year.⁸

The Netherlands is currently working towards the next generation DigiD solution called “DigiD hoog”. The solution will be more secure and will base on the Dutch identity card and driving license information [27]. The Netherlands also tries to integrate biometrical features into their national authentication scheme.

3 Research Design

In this research, we conduct a comparative case study on eIDAS implementation in the Netherlands and Estonia. For this purpose, we gathered an expert team and used action learning [10, 28] to compare the eIDAS implementation challenges of Estonia and the Netherlands and to find possible solutions to identified problems. Action learning [10, 28] is particularly well suited to research complex phenomena such as eIDAS [29].

One of the alternative research designs was a world café approach [30], but as the focus of this particular method is more on generating broader range of perspectives than to find answers, we found action learning more appropriate for, this study.

⁴ Smart-ID’s recognition as Qualified Signature Creation Device (QSCD), <https://www.smart-id.com/e-service-providers/smart-id-as-a-qscd/>.

⁵ Estonian eID statistics, <https://www.id.ee/?lang=en&id=>.

⁶ The Netherlands (DTF/eHerkenning) eID scheme notified under eIDAS, <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=74091935>.

⁷ Dutch Trust framework for Electronic Identification, <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=74091935>.

⁸ The Netherlands (DigiD) scheme pre-notified under eIDAS, <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=176620999>.

The research relies on an international collaboration between researchers, public and private sector experts from the Netherlands and Estonia. The Netherlands authority Digicampus⁹ coordinated and facilitated the cooperation. The Digicampus is an innovation hub that connects science, government, market players and citizens/users to shape future public services. Figure 2 illustrates action-learning-based collaboration between the Netherlands and Estonia [28].



Fig. 2. Project structure and participants.

As a result of the cooperation, two expert workshop sessions on (i) eIDAS implementation challenges and (ii) in service of finding possible solutions have been held at Tallinn University of Technology, Estonia, from November 18 to 21, 2019. Nine experts from Estonia and 14 experts from the Netherlands have been involved. Table 1 provides a detailed overview of the participants and their roles.

During the workshop sessions, we divided all participants into three groups presenting policy makers, the private sector and users. All groups consisted of participants from both countries. The first workshop took place on 19.11.2020, where experts shared their practical experience and challenges with the eIDAS implementation.

On the next day, the same groups continued working together and tried to find solutions to these challenges. After group work on both days, each group presented its result and the other groups had an opportunity to supplement it.

⁹ Digicampus homepage, <https://www.dedigicampus.nl/>.

Table 1. Project structure and participants.

Estonia		The Netherlands	
Organization	Role	Organization	Role
Information System Authority	Head of eID department	Ministry of the Interior and Kingdom Relations	Policy officer (digital government)
	Product owner (eIDAS cross-border usage)		Senior advisor (member of the Dutch eIDAS team)
Police and Border Guard Board	Adviser-expert (eIDAS implementation, auditing)		eHerkenning project manager
	Chief-expert (eIDAS SPOC)	Strategic advisor	
Ministry of Economic Affairs and Communications	Adviser (SDG national coordination)	Municipality of Den Haag	Adviser (digital transformation)
SK ID Solutions AS	Lawyer (trust services, eIDAS, ETSI EN standards, national law)		Product owner (digitalization and authentication)
TalTech	Full Professor of Information Systems (e-governance and technologies)	TU Delft	Senior researcher Master students (2)
		Agentschap Telecom	Supervision of eIDs
		ICTU	Sr advisor Program manager
	Researcher (eIDAS framework)	Netherlands Enterprise Agency	Product owner (International Access)
Researcher (public acceptance of eID)	Private sector representatives	Four persons	

4 Findings

In this section, we present our research findings from three different perspectives: policy maker, service provider and user perspective. We focus mainly on the eIDAS implementation problematics and do not reflect the discussions regarding other relevant topics more or less related to eIDAS, like applicability of the once-only principle (OOP) [31] or the implementation of the SDGR regulation.

4.1 Challenges and Solutions from the Policy Maker Perspective

From the policy maker perspective, we identified challenges related to the following issues: *implementation, (national) legislation, interpretation, compliance and communication.*

A crucial eIDAS implementation barrier is the lack of the EU common identifier. It is still not possible to use national eIDs and digital signatures for EU services. Particularly problematic is when users would like to act on behalf of others despite of sufficient legal grounds. The experts found that it is important to find a workaround or initiate further discussions on the EU common identifier to overcome this barrier. These challenges concern both natural and legal persons; and the topic should be added to the further research agenda.

The experts found that slight differences in the national laws complicate the uniform eIDAS implementation process in the EU. For example, according to the national laws, the actions that minors are allowed to perform varies from country to country. This affects, in particular, the establishment of cross-border services.

From the legal person's perspective, eIDAS allows for company eIDs without persons attached to it. This raises several practical questions. For instance, how to make it possible that a person is allowed to act on behalf of a company? How to use a legal person eID across borders? It is important to define all the issues related to legal persons separately and provide feedback to the eIDAS review process.

Representatives of the policy maker group considered interpretation of the eIDAS regulation as a crucial challenge. For example, Article 6 (that regulates mutual recognition of eIDs) is ambiguous. In addition, it is not clear how to map existing technologies to eIDAS assurance levels and how to assess their risks.

The experts identified the following shortcomings at the level of compliancy:

- not all member states offer eID;
- lack of supervision;
- the EC executes its supervisory role only weakly;
- the member states do not always accept each other's eIDs (e.g. Germany/Estonia);
- it lacks a framework for conformity assessment on the EU-level;
- There are no common rules for supervisory bodies.

The creation of assessment guidelines for auditors would help significantly to overcome the previously identified issues. Another solution that experts considered was the integration of ethical hacking into the eIDAS framework in order to improve existing requirements.

Finally, the experts agreed that the current SDG (Single Digital Gateway) program should have a stronger link to the eIDAS regulation and implementation activities. They also noted, that communication activities (i.e., why it is important to implement eIDAS) from the EU side should be improved.

4.2 Challenges and Solutions from the Service Provider Perspective

From the service provider perspective, we identified challenges related to the following issues: *collaboration, compliancy, reputation, change management, notification and record matching*.

The experts found a crucial challenge that lies on a co-operational level. It is not clear how to combine different competences in case of incidents (problem ownership issue). Applying EU wide user testing and meta-research on the cross-border collaboration level would help to solve this issue.

There exist no common rules for service providers on how to comply with the eIDAS regulation. Service providers are unsure, how to test their systems, i.e. how to understand whether their systems are compliant or not. Therefore, a standardized test framework with test data would be very helpful (e.g., a standard backward-compatible API).

Different change management issues complicate the eIDAS implementation process. It is not easy to keep up with changing standards and regulations. Often, changes are unpredictable and require remarkable additional investments. Misinterpretation of requirements can cause unnecessary additional work and costs. The experts found that eIDAS could be provided as a service for all public and private authorities (e.g. “spin a node and go”). Exploiting the World Wide Web Consortium (W3C), decentralized identifier (DiD) as a unique identifier (UiD) seems promising, but needs further in-depth research.

The eIDAS regulation provides no guidelines and standards for unique identifiers of persons (i.e., mandatory vs. free attributes, registration of foreign identities, tracking etc.). There is also lack of a common architecture API platform. The experts found that use of decentralized identifiers and identity linking would help to overcome the previously identified issues.

Notification of private sector solutions is a complex topic. Private sector service providers has no access to the data in the scope of the eIDAS regulation. However, fully automated and cross-border services need person related data. In this case, a common understanding of trust and privacy models plays an important role.

The experts found, that reputation is also an important topic, dependent on the reputation of all participants acting inside the eIDAS framework. The eIDAS framework is based on trust, but the meaning of *trust* differs in different cultures.

4.3 Challenges and Solutions from User Perspective

The user perspective covers a variety of challenges starting from usability to security and privacy concerns.

Accessibility and user experience (UX) of cross-border services needs improvement through additional guidelines, templates, examples, UX tests, experience and sharing of best practices. The same service may have a completely different user experience in different countries. This makes it difficult to find the right services abroad. In this case, standardized service portals that direct people to the right place, would be helpful. The experts also discussed language support and semantics problems that can be overcome by organizing learning courses and by describing step-by-step use cases.

From the security perspective, users have to understand whether they are using qualified services to avoid possible “man in the middle” attacks. Security awareness can be increased by developing guidelines, templates, sharing best practices and educating users continuously.

There is also a need for a governance framework and clear role division, as users often do not know whom to contact in case of technical error, usability problems or other relevant questions.

The experts discussed how to avoid errors and how to deal with service continuity when certificates become invalid. A would help solving this issue.

Finally, the experts found the current cross-border roles and mandates are insufficient. For example, users are unable to act on behalf of a legal person that they represent. From that perspective, the experts suggested that the scope of eIDAS regulation should contain the procedures related to the legal persons. They also proposed introduction of an EU common identifier.

5 Discussion and Recommendations

Based on our research results, it is clear that eIDAS implementation process is challenging from various perspectives. Policy makers, service providers and users have different expectations and needs. Based on the workshop results, where experts offered solutions to the eIDAS implementation challenges, we identified five main themes that all groups mentioned during the workshops in one or another way. These five common challenges are:

- compliance issues;
- interpretation problems;
- different practices in member states;
- co-operation and collaboration barriers;
- legal persons and their representation.

Compliance issues include insufficient guidelines (and supervision) for public service providers, private sector service providers and conformity assessment bodies. In this situation, parties start to interpret the requirements according to their practice; and this leads to the problem of different interpretations, starting from the usage of terminology to system usability issues. All identified challenges create additional communication and collaboration barriers between service providers and users as well as between EU member states.

Another interesting finding from the workshops is that most of the challenges are related with cross-border service provision rather than eIDAS implementation inside countries. Existing rules and requirements support the implementation of eIDAS inside member states, but are not sufficient to support the EU-wide implementation.

Table 2 provides detailed summary of eIDAS implementation related challenges and solutions from all three perspectives.

During the workshop, the experts discussed various options to overcome existing challenges and improve the eIDAS implementation process. Therefore, European Commission could consider the following proposals in the upcoming eIDAS review process:

- options to implement a common EU identifier;
- regulate the identification of users so that they can act on behalf of others when legally required;
- specify the regulation with respect to legal persons;
- clarify the terminology of the eIDAS regulation;

Table 2. Summary of eIDAS related challenges and solutions.

	Category	Challenges	Solutions
Policy maker	Implementation	No EU wide identifier	Workaround
		Acting on behalf of others	Workaround
		National eIDs/digital signatures are not usable for EU services	Initiating further discussions on the EU common identifier
	Legislation	Different legal practices in Member States	Creation of assessment guidelines for auditors
	Interpretation	Differences in the interpretation of the eIDAS articles	Creation of assessment guidelines for auditors
	Compliance	Different shortcomings	Creation of assessment guidelines for auditors
	Communication	eIDAS implementation importance	Communication plan
Service provider	Collaboration	Problem ownership issue	EU wide user testing
			Meta-research on the cross-border collaboration
	Compliance	Compliance of service providers	Standardized test framework with test data
	Change management	Changing regulations, standards	eIDAS provided as a service
	Notification	Notification of private sector solutions	Common understanding of trust and privacy models
Record matching	No standards for unique identifiers/lack of common architecture	Common architecture API platform	
		Use of decentralized identifiers	
		Identity linking	
User	Usability	UI consistence usage	Additional guidelines, templates, examples, UX testing, experience and sharing of best practices
		Accessibility to e-services	
		Different countries have different practices	Standardized service portals
	Helpdesk/ Support	User support in case of errors	Clear role division
		Language support and semantics	Courses, step-by-step use cases
	Security	Possible “Man in the middle” issue	Guidelines, templates, sharing best practices, user education
		“Dirty error” issue when certificates are invalid	Central monitoring service

- clarify often misinterpreted articles in the eIDAS regulation;
- develop common assessment guidelines for auditors;
- develop a standardized testing framework;
- provide eIDAS as a service;
- create a common monitoring system for cross-border transactions;
- develop a framework of standards for cross-border services.

Not all of these proposals and activities presume changes in the eIDAS regulation. Many of these initiatives require further discussion between the member states and more detailed analysis by the responsible organizations.

6 Future Directions

Current research is a part of a larger research project regarding the eIDAS, which aims to improve its compliancy assessment model. To develop this model we analyze and compare the eID schemes of different member states and their eIDAS implementation practice.

During this particular research, we identified various topics and questions that need further in-depth research and analysis. For example: requirements and preconditions for the application of a common EU identifier; creation of assessment guidelines for auditors, implementation of EU wide user-testing environment; cross-border service provision; collaboration between public service providers and private sector service providers. These topics will address in the scope of further research actions.

We hope that the outcome of the whole study is a valuable tool for the public and private sector eID service providers and auditors enabling more transparent and comparable assessment of different eID schemes. Moreover, our research results will be the basis for the further universal applicability analysis of the eIDAS principles while implementing SDGR regulation and establishing secure e-service provision between EU and third countries.

7 Conclusion and Research Limitations

This study showed that different EU member states have faced similar problems in the eIDAS implementation process and that it is important to exchange practical experiences at the expert level.

From the limitations point of view, it is not possible to compile a complete list of challenges based on the experience of just two countries. Additionally, offered solutions and recommendations reflect the knowledge and experience of the experts who participated in the workshops. It means that there can be other alternative ways to overcome the identified challenges. However, we are convinced that the results indicate to major shortcomings and practical problems that member states face during an eIDAS implementation.

Based on our research results, it is possible to say that the focus of the member states (with respect to the implementation of eIDAS and in light of the SDGR regulation) has clearly shifted from a national level to a cross-border perspective. However, before taking this next step in terms of cross-border service integration it is important to ensure stable and interoperable network of eIDs.

We identified five challenging areas (compliance issues, interpretation problems, different practices in member states, co-operation and collaboration barriers, legal persons and their representation) in the eIDAS implementation process, which will inevitably affect the implementation of other related regulations.

This new situation requires a review of the existing EU eIDAS framework and procedures by the European Commission. Our study provides practical input to the eIDAS review process by identifying common challenges of the member states and making proposals to overcome them.

References

1. Vial, G.: Understanding digital transformation: a review and a research agenda. *J. Strateg. Inf. Syst.* **28**(2), 118–144 (2019)
2. Khatchatourov, A., Laurent, M., Levallois-Barth, C.: Privacy in digital identity systems: models, assessment, and user adoption. In: Tambouris, E., et al. (eds.) *EGOV 2015. LNCS*, vol. 9248, pp. 273–290. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22479-4_21
3. Pappel, I., Pappel, I., Tepandi, J., Draheim, D.: Systematic digital signing in estonian e-government processes. In: Hameurlain, A., Küng, J., Wagner, R., Dang, T.K., Thoai, N. (eds.) *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVI. LNCS*, vol. 10720, pp. 31–51. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-56266-6_2
4. European Parliament and Council: EU Parliament and Council regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC (2014)
5. The European Parliament: EU Parliament Resolution. Towards a Digital Single Market Act (2015/2147(INI) (2016)
6. European Parliament and Council: EU Parliament and Council Regulation (EU) No 2018/1724 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (2018)
7. Bhattarai, R., Pappel, I., Vainsalu, H., Yahia, S.B., Draheim, D.: The impact of the single digital gateway regulation from the citizens' perspective. *Procedia Comput. Sci.* **164**, 159–167 (2019)
8. Bharosa, N., Lips, S., Draheim, D.: Making e-government work: learning from the Netherlands and Estonia. In: Hofmann, S., Csáki, C., Edelmann, N., Lampoltshammer, T., Melin, U., Parycek, P., Schwabe, G., Tambouris, E. (eds.) *ePart 2020. LNCS*, vol. 12220, pp. 41–53. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58141-1_4
9. Yin, R.K.: *Applications of Case Study Research*. Sage, Thousand Oaks (2011)
10. Revans, R.W.: *ABC of Action Learning*. Gower Publishing, Ltd., Farnham (2011)
11. Berbecaru, D., Liyo, A., Cameroni, C.: Electronic identification for universities: building cross-border services based on the eIDAS infrastructure. *Information* **10**(6), 210 (2019)

12. Maliappis, M., Gerakos, K., Costopoulou, C., Ntaliani, M.: Authenticated academic services through eIDAS. *Int. J. Electron. Gov.* **11**(3/4), 386 (2019)
13. Klobučar, T.: Improving cross-border educational services with eIDAS. In: Rocha, Á., Adeli, H., Reis, L.P., Costanzo, S. (eds.) *WorldCIST'19 2019*. AISC, vol. 931, pp. 932–938. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16184-2_88
14. Berbecaru, D., Lioy, A., Cameroni, C.: Providing digital identity and academic attributes through European eID infrastructures: results achieved, limitations, and future steps. *Softw. Pract. Exp.* **49**(11), 1643–1662 (2019)
15. Gerakos, K., Maliappis, M., Costopoulou, C., Ntaliani, M.: Electronic authentication for university transactions using eIDAS. In: Katsikas, S.K., Zorkadis, V. (eds.) *e-Democracy 2017*. CCIS, vol. 792, pp. 187–195. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-71117-1_13
16. Vogt, T.: Die neue eIDAS-verordnung – chance und herausforderung für die öffentliche verwaltung in deutschland. *Inf. Wissenschaft Praxis* **67**(1), 61–68 (2016)
17. Tsakalakis, N., OHara, K., Stalla-Bourdillon, S.: Identity assurance in the UK. In: *Proceedings of WebSci 16 - The 8th ACM Conference on Web Science*. ACM Press (2016)
18. Pelikánová, R.M., Cvik, E.D., MacGregor, R.: Qualified electronic signature – eIDAS striking czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis* **67**(6), 1551–1560 (2019)
19. Engelbertz, N., Erinola, N., Herring, D., Somorovsky, J., Mladenov, V., Schwenk, J.: Security analysis of eidas – the cross-country authentication scheme in europe. In: *12th USENIX Workshop on Offensive Technologies (WOOT 2018)*. USENIX Association, Baltimore, MD, August 2018
20. Kutylowski, M., Hanzlik, L., Klucznik, K.: Pseudonymous signature on eIDAS token – implementation based privacy threats. In: Liu, J.K., Steinfeld, R. (eds.) *ACISP 2016*. LNCS, vol. 9723, pp. 467–477. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-40367-0_31
21. Tsakalakis, N., Stalla-Bourdillon, S., O'Hara, K.: Data protection by design for cross-border electronic identification: does the eIDAS interoperability framework need to be modernised? In: Kosta, E., Pierson, J., Slamanig, D., Fischer-Hübner, S., Krenn, S. (eds.) *Privacy and Identity 2018*. IAICT, vol. 547, pp. 255–274. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16744-8_17
22. Mocanu, S., Chiriac, A.M., Popa, C., Dobrescu, R., Saru, D.: Identification and trust techniques compatible with eIDAS regulation. In: Li, J., Liu, Z., Peng, H. (eds.) *SPNCE 2019*. LNICST, vol. 284, pp. 656–665. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21373-2_55
23. Lips, S., Pappel, I., Tsap, V., Draheim, D.: Key factors in coping with large-scale security vulnerabilities in the eID field. In: Kő, A., Francesconi, E. (eds.) *EGOVIS 2018*. LNCS, vol. 11032, pp. 60–70. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98349-3_5
24. Lips, S., Aas, K., Pappel, I., Draheim, D.: Designing an effective long-term identity management strategy for a mature e-state. In: Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) *EGOVIS 2019*. LNCS, vol. 11709, pp. 221–234. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27523-5_16
25. Tsap, V., Pappel, I., Draheim, D.: Factors affecting e-ID public acceptance: a literature review. In: Kő, A., Francesconi, E., Anderst-Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) *EGOVIS 2019*. LNCS, vol. 11709, pp. 176–188. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-27523-5_13

26. Tsap, V., Pappel, I., Draheim, D.: Key success factors in introducing national e-identification systems. In: Dang, T.K., Wagner, R., Küng, J., Thoai, N., Takizawa, M., Neuhold, E.J. (eds.) FDSE 2017. LNCS, vol. 10646, pp. 455–471. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70004-5_33
27. Roelofs, F.: Analysis and comparison of identification and authentication systems under the eIDAS regulation. Master's thesis, Radboud University, the Netherlands (2019)
28. Pedler, M.: Action Learning in Practice. Gower Publishing, Farnham (2011)
29. Zuber-Skerritt, O.: Action learning and action research: paradigm, praxis and programs. In: Effective Change Management Through Action Research and Action Learning: Concepts, Perspectives, Processes and Applications, vol. 1, p. 20 (2001)
30. Aldred, R.: From community participation to organizational therapy? World cafe and appreciative inquiry as research methods. *Commun. Dev. J.* **46**, 57–71 (2009)
31. Wimmer, M.A., Tambouris, E., Krimmer, R., Gil-Garcia, J.R., Chatfield, A.T.: Once only principle. In: Proceedings of the 18th Annual International Conference on Digital Government Research. ACM (2017)