TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Asa Kawamura

THE EUROPEAN UNION ELECTRONIC IDENTITY AND DATA PROTECTION IN THE FINNISH AND ESTONIAN LEGAL SYSTEMS

Bachelor's thesis

Programme HAJB08/17, specialisation EU and international law

Supervisor: Maria Claudia Solarte Vasquez, LLM, PhD

Tallinn 2023

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 10 770 words from the introduction to the end of conclusion.

Asa Kawamura

(signature, date)

Student code: 184007HAJB

Student e-mail address: askawa@ttu.ee

Supervisor: Maria Claudia Solarte Vasquez, LLM, PhD:

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Today many public and private services are being provided online in the European Union (EU) and across the world. Estonia and Finland have been a part of this digitalization of services and are nowadays highly digitalized societies. An important part of electronic services is to ensure them being secure and an electronic identity framework for confirming the identities, obligations and rights of the parties involved is a must for this. The regulation for guaranteeing these aspects are the electronic Identification, Authentication, and trust Services (eIDAS) Regulation for the electronic identity framework and the General Data Protection Regulation (GDPR) for the data protection. This bachelor's thesis presents a comparative analysis of data protection provisions related to electronic identity in Estonia and Finland. The aim of this study is to examine how the legal frameworks in both countries address the challenges and complexities associated with electronic identity and ensure compliance with the GDPR. The research methodology includes a review of relevant laws, regulations, guidelines, and scholarly literature related to electronic identity and data protection. The findings of this research contribute to a better understanding of the legal and regulatory landscape surrounding electronic identity and data protection in Estonia and Finland. By enhancing user privacy and compliance with data protection regulations, this study aims to promote trust and confidence in electronic identity systems, ultimately fostering the development of secure and user-centric digital ecosystems in both Estonia and Finland.

Keywords: eIDAS, eID, eSignature, electronic identification law, data protection, GDPR

INTRODUCTION

EU is working towards creating a system where every EU citizen has the possibility have a secure digital identity that can be used in all Member states, on the private and public sector both online and offline. This plan will be achieved with building on the existing rules created by the 2014 Regulation on electronic identification and trust services. The proposal for the new regulation on electronic identification and trust services focuses on creating a system that encourages cross-border use of electronic identity and trust services in both public and private sector. Currently only 14% of key public service providers across all Member States allow cross-border authentication with an e-Identity system.[1] Both Estonia and Finland are digitalized countries where legal identification is used in daily lives. Both countries have chosen different approaches to the implementation of the electronic identity regulation.

This thesis is about digital identity or electronic identity as it routinely required for transactions and use of services nowadays. The concept of digital identity is emerging and evolving as private and public services have been moving towards fully digitalized services and transactions.[2] What legal measures has Estonia taken to make the identity card a more popular tool for electronic identity than in Finland? And why have these two countries taken different approaches to this matter? The simple answer to this is that the Finnish law does not oblige the residents to have an identity card and the Estonian law does[3]. And how are the Finnish and Estonian governments anticipating the new European Union Digital Identity wallet to change the use of electronic identity. A key question regarding digital identity is data protection. What are the legal requirements for digital identity and data protection systems under EU laws, and how can organizations ensure compliance with these requirements? How has Finland and Estonia implemented these into national laws?

The topic of this thesis is electronic identity because of the EUDI Wallet that is currently being drafted, is a new and interesting aspect that will most likely affect majority of the population in

[1] *European Digital Identity*. (n.d.). European Commission. Retrieved October 10, 2022, from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[2] Sullivan, C. (2012). Digital identity and mistake. *International Journal of Law and Information Technology, 20*(3), p. 224

[3] Estonian Identity Documents Act**,** *Identity Documents Act–Riigi Teataja*. Retrieved February 7, 2023, from https://www.riigiteataja.ee/en/eli/504022020003/consolide#:~:text=%C2%A7%205.-,Identity%20document%20requirement%20for%20Estonian%20citizens,shall%20hold%20an%20identity%20card.&text=(2)%20An%20Estonian%20citizen%20specified,not%20hold%20an%20identity%20card

the EU. GDPR is not new, but very important topic since it protects people's privacy, which is a right in the European Convention on Human rights. The vital point of a or the 'right to privacy' is the protection against misuse of personal information. We want secure and safe access to online services, and GDPR is relevant in all online services, small and big.

Interestingly, there is not as much academic writing about electronic identity and related fields in Finland, unlike in Estonia. Even as Finland can be considered a highly digitalized community, much can be learned from Estonia. When searching online for research on electronic identity in Finland, the Finnish literature concentrates on how to include the use of electronic identity in good governance. Use of electronic identity in public services is important, but not the sole purpose for electronic identity. Estonia and Finland were chosen for the countries to be examined is because Estonia is one of the leading countries in electronic identity and other electronic society[4] and while Finland is also a digitalised society it is not as advanced as Estonia. Therefore, as an interest point neighbouring countries in the EU with little population, provide an interesting basis for comparison. Similar, but still in many ways different.

The focus of this thesis is the legal framework and not the technical solution. The literature for the thesis is from Edilex[5], the search portal Primo[6], the official websites of EU, Estonia and Finland, Google Scholar and for the general information Google Search Engine. The methodology for this thesis is qualitative data analysis to study the communication of legislation and the effects of language in the legal texts, for electronic identity.

This study examines the digital identity and data protection legal frameworks in the EU, Finland, and Estonia, highlighting their differences and exploring their impact on the implementation and use of digital identity. By analysing the legal requirements, rights, and safeguards in these frameworks, this research aims to provide insights into the legal factors that shape the adoption, functionality, and security of digital identity systems in these regions.

[4] 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*.

[5] *Edilex Legal Information Service*. (n.d.). EDILEX. Retrieved April 8, 2023, from https://www.edilex.fi/tietoa_palvelusta/english

[6] *Tallinn University of Technology Library portal Primo*. (n.d.). Tallinn University of Technology Library Portal Primo. Retrieved February 4, 2023, from https://tutl-primo.hosted.exlibrisgroup.com/primo-explore/search?vid=372TUTL_VU1&sortby=rank&lang=en_US

The structure of this thesis four main chapters, after the introduction and it consists of electronic identity, electronic identity in the European Union, comparison of Estonian and Finnish legislations and finally the conclusion.

The first chapter after the introduction is about the concept of electronic identity, emphasizing its significance in the digital age. This chapter has three sub-chapters, the first being about identity and signatures, the focus is on the relationship between identity and signatures in the context of electronic transactions. It explains how electronic identity serves as a foundation for digital signatures, enabling authentication and verification of individuals in online interactions. And in the other sub-chapter, electronic identity framework is discussed, explaining the basis of why it is important. The last part of this chapter explores the crucial aspect of data protection in the context of electronic identity. It describes legal and regulatory frameworks, such as the General Data Protection Regulation (GDPR), that govern the handling and processing of personal data in electronic identity systems.

The next chapter focuses on the state of electronic identity in the European Union (EU). It also has three sub-chapters, where the first discusses the future of electronic identity within the EU, including the proposal for a European Digital Identity framework. The next two sub-chapters provide insights into the electronic identity landscapes of Estonia and Finland, highlighting their respective approaches and initiatives.

In the last chapter before conclusion, a comparative analysis is conducted, examining the similarities and differences between the legislations and approaches to electronic identity in Estonia and Finland. It highlights key aspects such as the regulatory frameworks, data protection measures, and initiatives taken by each country.

And finally, the conclusion summarizes the main findings and insights from the discussion. It emphasizes the importance of electronic identity and data protection in the context of a rapidly evolving digital landscape. It also underscores the significance of Estonia and Finland as countries to observe and learn from in terms of their advancements in electronic identity and their approaches to regulation.

2. Electronic identity

The starting point to understanding what digital identity is to start from the definitions of identity, how it is established and how are signatures related to the topic. As de Andrade said: "Electronic Identity (elD) is the backbone of modern communications and transactions in the digital world".[7] This chapter defines the definitions' of identity, digital identity, signature, electronic signature and why they are important. In essence digital identity is a product that contains data of the user that can be used for electronic services by concluding the contracts with an electronic signature.

2.1. Identity and signature

The right to identity is constructed of several rights and these are established in several human rights treaties. For an example the right to identity is established in the Universal Declaration of Human Rights (UDHR), where it is declared that everybody has a right to judicial personality[8], and the International Covenant on Civil and Political Rights (ICCPR) declares that everybody has the right to have a name[9], be registered right after birth[10] and have a nationality[11]. As there is no unified definition for identity, these aspects that are guaranteed for people in the human rights can be considered components of one's identity. In 2015 United Nations (UN) included legal identity as a global development target in their Sustainable Development Goals (SDGs).[12] There however is not an established definition on what legal identity is in the SDGs nor in the international law.[13]

Judicial identity establishes the recognition as a person before the law, enables a person to assert their rights, to enforce contracts, or to assert or defend a case in court.[14] Registration at birth gives a person a proof of their identity. A legal identity is the recognition of a person's identity in law and identity is simply what a person is.[15] While there is not a universal definition for legal identity,

[7] de Andrade, N. (2013). Electronic identity for Europe: moving from problems to solutions. Journal of International Commercial Law and Technology, 8(2), p. 104
[8] UN General Assembly. (1948). Universal declaration of human rights (217 [III] A). Paris. Art. 6
[9] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) Art. 24(2).
[10] ICCPR, Art. 24(2).
[11] ICCPR, Art. 24(3).
[12] Sperfeldt, C. (2022). Legal identity in the sustainable development agenda: Actors, perspectives, and trends in an emerging field of research. The International Journal of Human Rights, 26(2), p 217
[13] *Ibid.* p. 219
[14] Manby, B. (2021). The Sustainable Development Goals and 'legal identity for all': 'First, do no harm'. World Development, 139, 105342. p 2
[15] *Ibid. p. 3*

one definition is that legal identity is "the recognition of a person's existence before the law, facilitating the realisation of specific rights and corresponding duties"[16]. Manby states that it is important to differentiate legal identity and identification.[17] Identification is something that is used to establish a person's identity and to differentiate the person from others. Identification can be stored in a register and then confirmed by issuing some type of credential, i.e., passport, as a proof.[18] Differentiating legal identity and identification is important because people have rights whether they have identification or not.[19] Many rights however are tied to having a proof of identity and this is why identification proof of legal identity is important, because it is necessary in order to access certain rights, services and protections, such as accessing health services, opening a bank account, or graduating from school.[20]

A technology book about identity describes digital identity followingly: "*A digital identity contains data that uniquely describes a person or thing (called the subject or entity in the language of digital identity) but also contains information about the subject's relationships to other entities* ."[21] A digital identity in other words is something that exists in the digital realm and has the required information for the person's identification. And this digital identity can be used in digital services, to make contracts. Just as we make contracts and other legal acts in person, by expressing our will with a signature, we can use our digital identity by expressing our will with digital signatures.

It is important to differentiate the definitions of electronic identity and electronic signature. This is important because although these two have different functions, they are not always clearly differentiated. This can make analysis difficult and potentially hinder our ability to see alternative solutions.[22] People have been using signatures for centuries in various forms for multiple different purposes[23], therefore it is important to define what it means in the topic of e-ID and law.

---

[16] González López, L., Brøndsted Sejersen, T., Oakeshott, N., Fajth, G., Khilji, T., & Panta, N. (2012). Civil registration, human rights, and social protection in Asia and the Pacific. *Asia-Pacific Population Journal, 29*(6), 75-97. p. 77
[17] Manby (2021) p. 3
[18] *Ibid.*
[19] *Ibid.*
[20] Sperfeldt (2022), *supra nota 8*, p 220
[21] Windley, P. J. (2005). *Digital Identity: Unmasking identity management architecture (IMA)*. " O'Reilly Media, Inc.". p. 8
[22] Lentner, G., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government, 10*(1), p 10
[23] https://www.historyofinformation.com/detail.php?id=2239 accessed 30. Jan 2023

In 1980s there was no universal legal definition for signature.[24] However, it was acknowledged that signatures serve two purposes; the identification of the signatory and expressing the will to accept the contents of the document.[25]

As there are many ways to sign a physical document, different ways to mark, e.g., stamping, writing, and engraving, there are different styles of electronic signatures. Different methods of electronic signature can be using an electronically penned signature, typing a name in an e-mail, scanning a handwritten signature or many other ways.[26] Digital signature on the other hand is something that is in a digital form, and often has a certain standard of technology.[27] Many jurisdictions recognise a hierarchy of digital signatures, depending on the level of verification of the data.[28]

There may be differences in the terms used, but most electronic signature laws acknowledge the variances between the four levels, the simple electronic signatures (SES), advanced electronic signatures (AES), digital signatures and qualified electronic signatures (QES).[29] The first level being simple electronic signatures is used as an umbrella term that contains any electronic signature. The second level where advanced electronic signatures have certain requirements for signatory identification and authentication. Thirdly, digital signatures meaning those that have certain encryption technologies for added security. And lastly qualified electronic signatures that meet certain government-licenced or government-mandated requirements for the authentication, identifiation of signatories and tamper-proofing, such as encryption and dual-factor authentication.[30]

The current regulation in force concerning electronic identification in the EU, the eIDAS Regulation defines electronic identification followingly in the Article 3: "*the process of using*

[24] Antoine, M., Brakeland, J., Eloy, M., & Poullet, Y. (2001). Legal Requirements Facing New Signature Technology. In Advances in Cryptology — EUROCRYPT '89 (Lecture Notes in Computer Science, pp. 273-287). Berlin, Heidelberg: Springer Berlin Heidelberg. p. 274
[25] *Ibid.*
[26] Determann, L. (2021). Electronic Form Over Substance: ESignature Laws Need Upgrades. The Hastings Law Journal, 72(5), p. 1394
[27] *Ibid.*
[28] *Ibid.*
[29] *Ibid. p. 1395*
[30] *Ibid.*

person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person"[31].

2.2 Electronic identity framework

When talking about anything as abstract as identity, and everything that is included with it, it is important to define the terms, to understand what they are. Especially as adding the "electronic" aspect to these terms complicate the topic even more. When we talk about electronic identity, it is important to understand the basis of the field it exists in. The electronic identity (e-ID) is created by electronic government (e-government).

In this thesis the most important aspect of government is the functioning of government, particularly in the field of creating the rules and regulations of government and managing the state affairs. Since this is a legal thesis, the focus is on the rule-of-law, creating the framework and basis for the e-ID. Saarenpää focuses that government is an information process, as the moment we interact with government, a process that is legally regulated begins.[32]

Digital government is a government that is facilitated by information and telecommunication (IT) technologies and the internet.[33] Digital government has two spheres, where electronic government is one part of it and electronic democracy the other.[34] E-government assesses the needs of governing all the levels of services.[35] The primary concerns in e-government are providing broad access to transactional and information services to the citizens, as well as efficiency in administration.[36] As a society we require a proper government framework, that includes in the field of electronic government to process various activities. Therefore, legal framework is an essential pillar to e-government.[37] As the focus of this thesis is the legal point of view, the definition of government will comprise of the constitutional state. The government must comply with the

[31] The European Parliament and the Council of the European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 (eIDAS Regulation No 910/2014)
[32] Saarenpaa, A. (2003). A Legal Framework for e-Government. ELECTRONIC GOVERNMENT, PROCEEDINGS, 2739, p. 377
[33] Khalid S. Soliman John F. Affisco, Affisco, & Soliman. (2006). E-Government. Bradford: Emerald Group Publishing Limited. p. 8
[34] *Ibid.*
[35] *Ibid.*
[36] *Ibid.*
[37] Saarenpaa (2003). p. 378, *supra nota 11*

procedural and legislative framework of the constitutional state and the same applies to the electronic government.[38]

The benefit of e-government has been noted as facilitating collaborative and participatory engagement of citizens, other governments and businesses as well as reducing the cost of services.[39] The aim of e-Government is to encourage participation and inclusive process of decision-making and governance by bringing together public sector, civil society, international partners, and other stakeholders and benefiting this way the community.[40]

2.3 Data protection

Another aspect of electronic identity is data protection. People are interested in protecting their identities, both online and offline, and for a good reason. A person's identity is an important tool for the person themselves, but other people can take advantage of it also and do harm. EU takes data protection very seriously and that is why the EU has a strict regulation on data protection, which many are familiar with, The General Data Protection Regulation (GDPR)[41]. The GDPR has been in force since May 2018 and is a significant step in the development of European privacy framework.[42] Before the GDPR the EU had a Data Protection Directive (DPD)[43] that was effective from December 1995 until the GDPR came into force. The DPD was the basis of GDPR and unified MS's laws on privacy.[44] The GDPR guarantees the citizens and residents of the European Union to have the right to ownership of their own data and it is required to ask for permission for commercial or other use.[45]

Personal data which is strongly linked to a person's identity, means in the context of GDPR "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an*

[38] *Ibid. p. 379*
[39] Bwalya, Stephen M. Mutula, & Mutula. (2014). E-Government. De Gruyter. p. 4
[40] *Ibid. p. 5*
[41] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR) 2016/67)
[42] Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research, 59*(6), p. 703
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[44] Sharma, S. (2019). *Data Privacy and GDPR Handbook*. John Wiley & Sons. p. 33
[45] *Ibid.* p. 18

identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[46].

The ideology behind the GDPR is guided by philosophical approach that privacy is a fundamental human right as it is also enforced by the Charter of Fundamental Rights of the European Union (CFR)[47].[48] The CFR includes the respect for private life in the Article 7 and protection of personal data in Article 8. There are two main features to the GDPR personal data protection, which are data security mandates and privacy rights.[49] Both which are important aspect with electronic identity, especially in the case of privacy rights for those individuals using it and data security mandates for the entities that collect the data. The most important privacy rights in the GDPR are firstly the right to explicit content, to opt in for data collection, second the right to be forgotten and thirdly the right to data portability.[50] The GDPR data security mandates state how the data collectors must store, process and share the necessary data, but also that the data collectors must be proactive in ensuring that the data is private by design.[51]

There are seven data protection principles in the GDPR that are stated in the Article 5. Those are 1. lawfulness, fairness, and transparency, 2. purpose limitation, 3. data minimization, 4. accuracy 5. storage limitation, 6. integrity and confidentiality, and 7. accountability.

However, there are some issues with the compliance of GDPR in practise. As organizations are only required to demonstrate compliance with the GDPR when there is suspicion of a violation or when a data subject lodges a complaint[52]. The challenge of complying with the GDPR is not due to a lack of technical solutions or mechanisms, but rather because these solutions are often designed and implemented with a centralized client-server architecture mindset. This irregular verification of GDPR compliance has raised concerns about the lack of transparency in the process.[53] Blockchain (BC) technology is suggested as a remedy for this.

[46] General Data Protection Regulation (GDPR) 2016/67, Art4(1)
[47] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION 2012/C 326/02 (CFR)
[48] Goddard, M. (2017) p. 703
[49] Ke, T. T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*. p. 1
[50] *Ibid.* p. 2
[51] *Ibid.*
[52] GDPR Art. 33, Art. 13–15
[53] Park, C., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, *15*, p. 1746

In simplicity, blockchain technology is as follows. Blockchain technology is a decentralized and unchangeable database made up of a growing list of blocks. This database, called a blockchain, keeps a record of all transactions between different entities in a network.[54] Once information is recorded in a block in a blockchain, it cannot be changed in the past without affecting the entire chain. This ensures the consistency and agreement among the network nodes. The concept of blockchain was first introduced in Bitcoin in 2008. Bitcoin is a cryptocurrency that securely transacts digital currency and solves the issue of "double spending" without relying on a trusted third-party.[55]

One example of BC being a tool for better data control is transparency. BC can allow data owners to impose data usage consent, ensure that only designated parties can process personal data, and to log all data activities in an immutable distributed ledger using smart contract and cryptography techniques. By honestly participating in the platform, a service provider can be endorsed by the blockchain network that it is fully GDPR-compliant; otherwise, any violation is immutably recorded and is easily figured out by associated parties.[56]

3. Electronic Identity in the European Union

Electronic signature was introduced in 1999 with the Directive on a community framework for electronic signatures (eSignature Directive)[57]. It was a crucial step to enable a transition to fully electronic documents to introduce electronic signature into the legal framework.[58] The early hopes of quick replacing of paper documents with digital versions transpired to being optimistic.[59] It was expected that the 2014 Regulation on electronic identification and trust services for electronic

[54] *Ibid.* p. 1748
[55] *Ibid.*
[56] *Ibid.*p. 1746
[57] The European Parliament and the Council of the European Union, Directive 1999/93/EC on a community framework for electronic signatures, 1999
[58] Kutylowski, M., & Blaskiewicz, P. (2023). Advanced Electronic Signatures and eIDAS – Analysis of the Concept. Computer Standards and Interfaces, 83, 103644. p. 1
[59] *Ibid.*

transactions in the internal market (eIDAS Regulation)[60], which replaced the 1999 Directive in 2016, would push the process forward. eIDAS was expected to replace the national regulations that were not always compatible.[61]

The beginning of electronic commerce and electronic signatures began in 1997 when the Commission of the European Community started working on a Directive in order to pre-empt MSs from enacting national legislations.[62] Before the 1999 eSignature Directive came into force in January of 2000 and established the recognition of electronic signatures, only hand-written signatures were legally valid in the EU.[63] The aim of the 1999 eSignature Directive was to create a Community framework for the use of electronic with the free movement of services of products in the EU cross-borders.[64] The eSignature Directive led to almost every MS having a national regulatory framework for electronic signatures.[65] The eSignature Directive was intended as an essential and important new legal standard for the regulation of electronic signatures and MSs had to implement it into the national laws before the 19th of July in 2001.[66] The intentions for this eSignature framework was to ensure trust and security in electronic commerce and communication, as well as to strengthen the general acceptance and confidence of the certification services to better the functioning of the internal market.[67]

The eIDAS Regulation came into effect on 1st of July 2016 and repealed the eSignature Directive rules on trust services.[68] The 2014 eIDAS Regulation established a new legal framework for ensuring the legal certainty of cross-border use of, i.e., website authentication certificates, e-seals, and e-signatures.[69] It is important to note the difference in statutes, as the 1999 eSignature Directive was a directive and the 2014 eIDAS Regulation is a regulation. The difference is

[60] The European Parliament and the Council of the European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 (eIDAS)
[61] Kutylowski, M., & Blaskiewicz, P. (2023), p. 1
[62] Determann (2021), *supra nota 10*, p. 1414
[63] *What is the legislation - esignature*. (n.d.). Retrieved March 3, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/What+is+the+legislation+-+esignature
[64] Kelm, S. (2005). On the Implementation of the 1999 Directive on Electronic Signatures. Digital Evidence and Electronic Signature Law Review, 2, 7-15. p. 7
[65] *Ibid.*
[66] Siems, M. M. (2002). The eu directive on electronic signatures a worldwide model or fruitless attempt to regulate the future. International Review of Law, Computers & Technology, 16(1), 7-22. p. 7
[67] *Ibid.* p. 8
[68] *What is the legislation - esignature*. (n.d.). Retrieved March 3, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/What+is+the+legislation+-+esignature
[69] *Ibid.*

important because of the effect on the national regulations was different as regulations require greater harmonization than directives.

The aim of the eIDAS regulation is to enable throughout the EU the citizens to be able to use their own MS's eID scheme to communicate and authenticate with other MS online services.[70] The eIDAS Regulation article 3 defines an eID scheme as a "*a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons*", whereas eID means is defined as "*a material and/or immaterial unit containing person identification data and which is used for authentication for an online service*"[71].

The MSs are allowed to notify one or multiple eID schemes concerning one or more eID means.[72] eID means are for an example European Digital Identity wallets or ID cards, that contain person identification data and which also is for online or offline service authentication, following the Regulation 2019/1157 on strengthening the security of identity cards[73].[74] As this cross border use of electronic identification means has been done on a voluntary approach the percentage of use has been lacking. As of 28th of April 2023, of the 27 EU member states 21 countries have notified their eID schemes, Germany being the first in 2017, Liechtenstein and Poland the latest this year.[75] Estonia has notified their eID scheme in the early group in November 2018 and Finland has not notified a scheme yet.[76] This is a major change from the year 2021 when only 14 MS's had notified at least one eID scheme.[77]

[70] Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F., & Ranise, S. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences, 12*(24), 12679.
[71] eIDAS Regulation (EU) No 910/2014, Art. 3.
[72] *Ibid.* p. 4
[73] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement
[74] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final (Proposal for eIDAS 2.0 (COM/2021/281 final))
[75]*Overview of pre-notified and notified eID schemes under eIDAS - eID User Community* -. (2019, September 13). Retrieved May 1, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
[76] *Ibid.*
[77] Proposal for eIDAS 2.0 (COM/2021/281 final)

3.1. Future of Electronic Identity in the European Union

The future of e-ID is being drafted currently. Among other digital developments in the EU, since October 2020 the European Council has been working on creating a new European Digital Identity with the goal of including a European Digital Identity Wallet (EUDI Wallet).[78] The current eIDAS Regulation does not require the MSs to notify an eID scheme, unlike in the Proposal for amending the eIDAS Regulation.[79] In the Proposal for amending the current eIDAS Regulation it is deemed that the current eID schemes notified by the MS's on enabling access to online public services to be too limited and inadequate.[80] According to the Proposal the public sector has not provided these services on a sufficient level, and that the majority of the needs of eID and remote authentication is used within the private sector, where the operators are required by the law to verify the identity of their customers, such as banking and telecom.[81]

There are several main objectives in the Proposal and one of them is establishing a framework for a European Digital Identity which means providing individuals and businesses with a secure and user centric digital identity solution. Another aim is interoperability and trust by enabling the recognition and acceptance of digital identities issued by different member states, in another word's harmonization is required. The goal for the eIDAS 2.0 is it to be voluntary and user controlled, the European Digital Identity is intended to be a voluntary and user-controlled system, this means that individuals would have the option to choose and use the European Digital Identity, while maintaining control over their personal data and designed to respect the GDPR data protection principles.

The proposed European Digital Identity Wallet is a service and a product where the user can store credentials, identity data and other attributes that are linked to their identity.[82] With this the user can provide the necessary data to relying parties on request and to use it for authentication both online and offline for services that are in accordance with the Article 6a.[83] The Article 6a contains requirements for the European Digital Wallet, such as security requirements and that the Wallet

[78] The General Secretariat of the Council. (2022, November 15). *A digital future for Europe*. The Official Website of the Council of the EU and the European Council. Retrieved April 23, 2023, from https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/
[79] Proposal for eIDAS 2.0 (COM/2021/281 final), *supra nota 15*, p. 7, 9
[80] *Ibid.* p.5
[81] *Ibid.*
[82] *Ibid.* p. 9
[83] *Ibid.*

must be free of charge for natural persons.[84] In the draft Regulation, it is also required that all MS' issue an EUDI Wallet under a notified eID scheme that follow common technical standards and pass a compliance assessment, the certification within the European cybersecurity framework which is established by the Cybersecurity act is voluntary in the Article 6a.[85]

Only EU-level intervention can lay down the harmonised conditions that ensure user control and access to cross border online digital services and an interoperability framework making it easy for online services to rely on the use of secure digital identity solutions, irrespective of where in the EU it has been issued or where a citizen resides. As largely reflected in the review of the eIDAS Regulation, it is unlikely that national intervention would be equally efficient and effective.

The proposal emphasizes the importance of cross-border access to digital services and aims to remove existing barriers by establishing a European Digital Identity that can be recognized and accepted throughout the EU. This would simplify interactions and transactions between individuals, businesses, and public authorities across member states.

The purpose of EUDI Wallet is to guarantee all EU citizens access to trusted digital identities, that allow the users to be in control of their own online presence and interactions.[86] The EUDI Wallet can be considered as a combination of Trust Services and several products, for the users to be able to securely store, obtain and request their information that can be used to accessing online services, sealing or signing documents electronically and presenting data about themselves.[87]

In the proposal it was explained that at the same time of the publishing of the proposal the Commission releases a Recommendation for the sake of harmonisation and avoiding creating fragmentation and barriers in the creation of eIDs. The European Commission adopted a Recommendation on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework[88] in June 2021, for the MS's to co-operate towards a Toolbox with a technical Architecture and Reference Framework (ARF), technical specifications and a set of

[84] *Ibid.*
[85] *Ibid.*
[86] *The European Digital Identity Wallet Architecture and Reference Framework*. (2023, February 10). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
[87] *Ibid.*
[88] Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework, C/2021/3968, *OJ L 210, 14.6.2021, p. 51–54*

common standards, and also a set of best practises and common guidelines.[89] In the Recommendation it was proposed that this is done through the eIDAS expert group.[90] The eIDAS expert group was established in 2014 by the Commission's Directorate General for Communications Networks, Content and Technology as a permanent and informal expert group for supporting the implementation of the eIDAS regulation.[91]

In the 2021 Recommendation the eIDAS expert group listed with a few first use case areas that are mobility and digital driving licence, health, secure and trusted online identification to access online services, digital finance, educational credentials and professional qualifications, and digital travel credential.[92] In the proposal it was pointed that as the current eIDAS regulation does not cover professional qualifications and medical certificates, for this reason it is difficult to ensure recognition of these in electronic form all across the EU.

The proposal acknowledges the significance of upholding individuals' privacy rights and complying with relevant data protection laws, such as the GDPR. Some of the main thoughts on data protection in the Proposal are described here. Privacy by Design and Default is emphasized, highlighting the integration of privacy considerations into the design of the European Digital Identity framework[93]. The default setting for any processing of personal data should prioritize privacy. User Control and Consent are key aspects addressed in the proposal[94]. It aims to empower individuals with control over their personal data, allowing them to provide explicit and informed consent for its use. The proposal promotes the principle of collecting and processing only necessary and proportionate data. The European Digital Identity framework should request and retain the minimum amount of personal data required for identification and authentication purposes[95]. Security and Integrity of Data are recognized as vital[96]. The proposal suggests implementing appropriate technical and organizational measures to safeguard personal data within the European Digital Identity framework, preventing unauthorized access, loss, or alteration of data. Data Portability and Interoperability are highlighted in the proposal[97]. It stresses the

[89] *Ibid.* 1. Objectives and definitions
[90] *Ibid.* 2. Process for developing a toolbox
[91] *eIDAS Terms of Reference*. (n.d.). eIDAS Expert Group (E03032). https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/42178/download
[92] Commission Recommendation (EU) 2021/946, p. 10
[93] Proposal for eIDAS 2.0 (COM/2021/281 final), *supra nota 15*, p. 45
[94] *Ibid.* p. 24
[95] *Ibid.* p. 18
[96] *Ibid.* p. 8
[97] *Ibid.* p. 4

importance of allowing individuals to easily transfer their digital identity data between different trusted providers. This enables individuals to maintain control over their data and choose the providers that best align with their preferences and requirements.

Overall, the proposal underscores the commitment to data protection principles within the European Digital Identity framework. It aims to ensure privacy, user control, minimal data collection, security, and data portability, fostering a trustworthy and user-centric digital identity ecosystem.

3.2. Electronic Identity in Estonia

As there is no universal definition for the definition of signature, there also is no legal definition for signature in Estonia.[98] According to the Estonian Explanatory Dictionary (Eesti keele seletava sõnaraamatu (EKSS)) a signature is a name written by one's own hand under the text. Therefore, a signature can be thought of as a graphic image, which a person has illustrated their name with letters. This dictionary definition can be used when defining the concept of signature. It must be noted that not any handwritten image can be considered as a legally binding signature. The important point of the dictionary definitions is that it is written in one's own handwriting, and this emphasizes that the signature must reflect the unique characteristics of the signer. When considering the purpose of a signature, when marking a legally binding signature, it is necessary for the signature to possess unique characteristics of the signer, for being able to verify that it was written by the same person on whose signature it claims to be. This is because signing a document create rights and obligations and is not merely a formality, opposing when marking one's belongings.[99]

The Estonian banks started issuing bank IDs in 1996.[100] Within a ten-year period, the plan was solidified, and numerous electronic systems were put in place. These systems included the electronic tax authority and cabinet in 2000, the "X-road" in 2001, and the electronic ID card with digital authentication and signature, as well as the 'digital school' in 2002. The Estonian central

[98] Saarmets, V. (2011). (Üld)tuntud ja tundmatu (ema)keel (2). Ajakiri Õiguskeel, (3), 1–23. Retrieved March 6, 2023, from https://www.just.ee/oigusloome-arendamine/oiguskeel/ajakiri-oiguskeel#item-13.
[99] *Ibid.*
[100] Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, *3*(1), p. 213

online citizen portal eesti.ee was introduced in 2003, followed by electronic municipal elections in 2005 and parliamentary elections in 2007. The digitization of the judiciary and notarial systems began in 2006, with mobile digital signatures and digital company registrations following in 2007. In 2008, digital healthcare was launched, and digital prescriptions became available in 2010.[101]

The Estonian Identity Documents act[102] obliges the people residing in Estonia to have an identity document in Chapter 2 Section 5 for Estonian citizens and Section 6 for EU-nationals and third-country nationals.

In Estonia Digital Signatures was first regulated by the Digital Signatures Act[103] (DAS) that came into force in December 2000. The law has been amended by the Electronic Identification and Trust Services for Electronic Transactions Act [104] (EUTS) that came into force in October 2016. EUTS consists of five chapters, which are: General Provisions, Trust Service and Trust Service Provider, Electronic Identification System, Supervision, and Implementing Provisions. The law has been amended thrice to be in better cohesion with the eIDAS Regulation, in 2019, 2021 and 2023.

DAS had specific requirements for digital signatures in Chapter I Section 2. DAS made digital signatures to be equally legally binding as handwritten signatures with Chapter I Section 2 subsection 1: "*A digital signature has the same legal consequences as a hand-written signature if these consequences are not restricted by law and if the compliance of the signature with the requirements of subsection 2 (3) of this Act is proved.*" The EUTS refers to the eIDAS Regulation for the definition of digital signature in Chapter 4 Section 24 and for the signatures before the EUTS came into refers to the DAS and eIDAS, and states that following requirements must be complied with:

> *"1) it is a data unit, created using a system of technical and organisational means, which is used by a signatory to indicate his or her link to a document.*
>
> *2) it is created by using a private key contained in a secure signature creation device to which the public key uniquely corresponds.*
>
> *3) with the system of using the digital signature it enables unique identification of the person in whose name the signature is given, determination of the time when the signature*

[101] Hoffmann, T. K., & Vasquez, M. E. D. (2022). The estonian e-residency programme and its role beyond the country's digital public sector ecosystem*. *Revista CES Derecho*, *13*(2), p. 184
[102] Identity Documents Act RT I 1999, 25, 365
[103] Digital Signatures Act RT I 2000, 26, 150
[104] Electronic Identification and Trust Services for Electronic Transactions Act RT I, 25.10.2016, 1

is given, and link the digital signature to data in such a manner as to preclude the possibility of changing the signed data or the meaning thereof undetectably after the signature is given.

4) it has been given by using a trust service certificate entered in the register of certification in compliance with the Digital Signatures Act."

Digitally signed documents must be accepted by all Estonian authorities.[105] In other words there are no limitations for the use of digital signatures in legal acts with the Estonian authorities.

In Estonia, the state issues different types of identity documents with the contact type smart card chip, the card is the size of a credit card.[106] These different types of ID-cards are the identity card, the residence permit card (RP card), and the nonphysical cards which are the digital identity card and the e-resident's digital identity card.[107] These cards are regulated in the Estonian Identity Documents Act (ITDS), Section 2.[108] The difference between the identity card and digital identity card is that the identity card is a card that has a physical form and the digital identity card is in a digital format and the same applies to the residence permit card. In the ITDS Chapter **5[1]** Section 20**[1]** Subsection 1 digital identity card is defined followingly "*A digital identity card is a digital document.*". The e-resident's identity card is for those who is not an Estonian citizen or a non-Estonian resident who currently has an identity card or residence permit card or who is applying for either of these cards.[109] These eID means, the ID card, RP card, Digi-ID, e-Residency Digi-ID, Mobiil-ID (until 01.07.2022) and Diplomatic identity card are notified eIDAS eID schemes.[110]

The identity card can be used to identify oneself to a machine electronically.[111] For an example the ID-card can be used in libraries for checking out books on self-service machines or in pharmacies

[105] Dang, T., Wagner, R., Küng, J., Thoai, N., Takizawa, M., & Neuhold, E. (2016). An Overview of Digital Signing and the Influencing Factors in Estonian Local Governments. In Future Data and Security Engineering (Vol. 10018, Lecture Notes in Computer Science, pp. 371-384). Switzerland: Springer International Publishing AG. p. 372
[106] Morgan, D., Parsovs, A. (2017). Using the Estonian Electronic Identity Card for Authentication to a Machine. In: Lipmaa, H., Mitrokotsa, A., Matulevičius, R. (eds) Secure IT Systems. NordSec 2017. Lecture Notes in Computer Science(), vol 10674. Springer, Cham. p. 175
[107] *Ibid.*
[108] Identity Documents Act RT I 1999, 25, 365
[109] *Ibid. Chapter **5[2]** Section **20[5]***
[110] *Estonia - eID User Community* -. (2018, November 7). Retrieved April 28, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia
[111] Morgan, D & Parsovs, A. (2017). *supra nota 21,* p. 175

to look up what drugs has the person been described to.[112] The digital identity card is only suitable for digital signing and authentication.[113]

Estonia has other types of eIDs, other than the digital identity card and the e-resident's identity card that can be used to authentication for accessing e-services. These are Mobile ID, Bank ID, Smart ID, username and password, PIN-calculator, and social media accounts.[114] In the 2017 study by Tsap et. al. the most popular authentication method was the ID-card.[115] A person can have multiple eID carriers at the same time, and the identity data is always the same on the carriers.[116]

The implementation of GDPR in Estonia is in the law Personal Data Protection Act (DPA)[117] that came into force in January 2019. The GDPR is directly applicable in all EU member states, including Estonia. However, each member state has the flexibility to implement certain provisions of the GDPR into their national laws. In Estonia, the GDPR is supplemented by the Estonian DPA, which provides additional details and provisions specific to the country.

The DPA sets out general principles and requirements for the processing of personal data, regardless of the specific context in which it is collected or used. This means that the provisions of the DPA apply to the processing of personal data associated with electronic identity, such as data collected during the issuance, use, or verification of electronic identification methods like national ID cards or digital authentication services. The DPA regulates how personal data is collected, stored, accessed, used, and shared, including in the context of electronic identity. It establishes the rights of data subjects, obligations of data controllers and processors, and mechanisms for ensuring data protection and security.

It's worth noting that the DPA works in conjunction with other relevant laws and regulations, such as the eIDAS Regulation and specific sector-specific laws, to ensure comprehensive data protection and privacy in the context of electronic identity in Estonia. The Estonian Electronic

---

[112] *Ibid.*
[113] Tsap, V., Lips, S., Draheim, D. (2020). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In: Kő, A., Francesconi, E., Kotsis, G., Tjoa, A., Khalil, I. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2020. Lecture Notes in Computer Science(), vol 12394. Springer, Cham. p. 159
[114] *Ibid.*
[115] *Ibid.*
[116] *Electronic Identity eID | RIA*. (n.d.). Retrieved March 22, 2023, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/electronic-identity-eid
[117] Personal Data Protection Act RT I, 04.01.2019, 11

Identification and Trust Services Act regulates the use of electronic identification within the country. It covers the provision of electronic identity services by both public and private sector entities. The law also outlines requirements for ensuring the security and protection of personal data associated with electronic identity. Additionally, the Cyber Security Act establishes requirements for the security of information systems and networks in Estonia. It encompasses provisions that address the protection of personal data processed in relation to electronic identity.

Estonia has developed a robust legal framework to safeguard personal data in the realm of electronic identity. These laws work together to ensure the protection and security of personal data in accordance with established regulations and guidelines.

Estonia has enacted specific laws and regulations in addition to the GDPR and the Estonian DPA to address data protection in different sectors or situations. These laws provide additional provisions and requirements for handling specific types of personal data. For example, the Electronic Communications Act[118] regulates electronic communications services in Estonia. It covers the processing of personal data by telecommunications operators and includes requirements for data security, confidentiality, and notification of data breaches. The Health Services Organization Act[119] governs the organization and provision of health services in Estonia. It includes provisions for processing personal health data, ensuring its confidentiality, security, and appropriate use within the healthcare sector. Additionally, the Public Information Act[120] regulates access to public information in Estonia. It addresses the processing of personal data by public authorities and aims to ensure transparency and openness in handling public information.

These laws complement the GDPR and the Estonian Data Protection Act, enhancing data protection measures in Estonia across various sectors and specific circumstances.

3.3. Electronic Identity in Finland

Again, as with the case with Estonia and the international field, there is no official definition for a signature. The definition of signature in the Dictionary of Contemporary Finnish (Kielitoimiston sanakirja) can be freely translated as a marking a document or any other similar, for the sake of

[118] Estonian Electronic Communications Act RT I 2004, 87, 593
[119] The Health Services Organization Act RT I 2001, 50, 284
[120] Public Information Act RT I 2000, 92, 597

confirmation.[121] In Finnish academic literature, the purpose of signature can be examined from multiple different angles, these being for an example identification, authentication, communication, will and proof.[122]

The purpose of a signature is the identification of the person who made the document or the person who is entering the contract, which means verification of the signatory's identity.[123] The identification purpose means that the reason for signing the document is to simply verify the person who signs the document, identifying the person. The authentication means verifying that the signature is connected to a person who created or sent the document. Signature's communicative function is that it communicates, who is the person who created the document or agreed to the document, to the person who receives or handles the document. The will function means that the purpose of the signature is to confirm afterwards that the expression of will, or resolution can be identified and connected to a specific person, or in other words signature expresses a specific person's will. A person expresses their will or commitment to the contents of the document. The proof function of a signature means that a signature can be used as evidence for the concluded judicial act or of the sender's identity if the other party denies the act at a later stage.

Interestingly having an identity document is not obligatory in Finland.[124] Identity documents are not mandatory in Finland, however there are some instances where it is required to show an identity document in order to receive the service but this can be avoided by requesting the police to identify the person.[125] Bank ID's are also accepted as authentication into private and public services.[126] A significant amount of service providers have transitioned to providing their services more online, rather than at physical locations.

In Finnish academic literature, a person's electronic identity means storing certain properties or data about a natural person in electronic form and using these properties or data for different purposes on electronic platforms.[127] On 16th of September 1996 the Finnish Ministries of Finance,

[121]Kielitoimiston sanakirja. 2022. Helsinki: Kotimaisten kielten keskus. URN:NBN:fi:kotus-201433. Verkkojulkaisu HTML. Päivitettävä julkaisu. Päivitetty 10.11.2022 [viitattu xx.xx.xxxx]. https://www.kielitoimistonsanakirja.fi/allekirjoitus

[122] Voutilainen, T. (2009). ICT-oikeus sähköisessä hallinnossa: ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita Publishing. p. 255

[123] *Ibid.*

[124] Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society*, *3*(1), p. 237

[125] 617/2009 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista

[126] *Ibid.*

[127] Voutilainen, T. (2009) p. 240

Transport, and Interior published a report on a person's electronic identity and identity card[128], this also might be the first Finnish official report on the topic of electronic identity and signatures.[129] In that report electronic identity is described as a tool that can be used for verifying one's identity.[130]

Elements that are included in electronic identity can be identifying information such as social security number, or other identifier, and biometric feature; a portrait, fingerprint, or a picture of eye's iris.[131] The identifying information or feature, must be unique and connect to only one specific person. A person's electronic identity can include also information about their family, their contact information and as a separate unit, information about their role, status, and authorization in a certain situation or activities.[132] These types of information has been recorded into national registries, such as population information system, trade register, association register, and register of guardianship matters.[133] The population information system is the basis of a natural person's electronic identity on people living in Finland, who have a social security number.[134] Electronic identity is a part of person's identity and a tool for legal capacity in an electronic environment.[135]

In Finland electronic signatures were first regulated in Act on Electronic Signatures that came into force on 1st of February 2003.[136] The law has been amended by the current Act on Strong Electronic Identification and Electronic Trust Services which came into force on 1st of September 2009.[137] The current law in force consists of eight chapters, which are General Provisions, Binding nature of the Act and processing of personal data, Strong electronic identification, Assessment of conformity, Provisions on trust services, Regulatory supervision, Miscellaneous provisions and Entry into force. The law has been amended multiple times, in years 2012, 2015, 2016, 2017, 2018, 2019 and 2021.

The 2003 Act on Electronic signatures define electronic signatures as "*data in electronic form which are attached to or logically associated with other electronic data and which serve as a*

[128] *Ibid.* p. 2
[129] *Ibid.* p. 243
[130] *Ibid.* p. 240
[131] Voutilainen, T. (2008). Sähköisen identiteetin käytöstä julkisessa hallinnossa. *Joensuun yliopisto: Edita,* p. 2
[132] *Ibid.*
[133] *Ibid.*
[134] *Ibid.*
[135] *Ibid.*
[136] Laki sähköisitä allekirjoituksista14/2003
[137] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009

method of authenticating the identity of the signatory". In 2003 there were three types of applications for e-signatures, and they were e-banking, e-government, and mobile e-commerce. E-banking was mostly for authentication, e-government was based on electronic ID cards and mobile e-commerce was issued by mobile operators. The eID card can be used in several e-government services and contains qualified certificates. The eSignatures are equally binding as handwritten signatures.[138]

In 2019 the Finnish Ministry of Finance published a study on electronic identity that they requested to be researched by the Population Register Centre.[139]

As GDPR regulation is directly applicable in all EU member states it applies also directly to Finland. However, as the member states have some flexibility in implementing certain provisions of the regulation into their national laws. In Finland, the GDPR is supplemented by the Finnish Data Protection Act (DPA)[140], which provides additional details and provisions specific to the country. The Data Protection Act came into force in January 2019 and has undergone revisions in the years 2020, 2022 and 2023 to align with changing data protection requirements and to complement the GDPR.[141]

In addition, there are special laws in Finland addressing data protection in certain sectors or situations that provide additional provisions and requirements for personal data processing. These are for an example the Act on the Openness of Government Activities[142] which includes provisions of processing personal data by public authorities and ensures that individuals have access to information held by public bodies, Act on the Protection of Privacy in Working Life[143] which includes rules in for employers regarding the collection, use, and retention of employee data and Act on Electronic Communications Services[144] which includes provisions related to the processing of personal data by telecommunications operators, such as requirements for data security, confidentiality, and notification of data breaches.

---

[138] Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., & Van Eecke, P. (2003a). *The legal and market aspects of electronic signatures* (C 28.400). Interdisciplinary centre for Law & Information Technology. Retrieved March 31, 2023, p. 187.
[139] Mitrunen, J., Salovaara, T., & Viskari, J. (2019). Sähköinen tunnistaminen: Selvitys nykytilasta sekä-kehittämistarpeista.
[140] Tietosuojalaki (1050/2018) https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf
[141] *Ibid.*
[142] Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
[143] Laki yksityisyyden suojasta työelämässä 13.8.2004/759
[144]Laki sähköisen viestinnän palveluista 7.11.2014/917

4. Comparing the legislations with similarities and differences

The Finnish ID-card's signature is an electronic signature, which is distinct from a digital signature and is not recognized as equivalent to a handwritten according to Estonian legislation.[145] The electronic signatures produced by the Finnish ID-card have an AdES/QC signature level, which means they do not meet the criteria for the highest signature level defined by eIDAS. Consequently, a signature made with the Finnish ID-card is not equivalent to a handwritten signature, and DigiDoc4 will display the following warning regarding the signature level: valid (with limitations).[146]

In terms of legal definitions of signatures, Estonia and Finland have different definitions. According to the Estonian Explanatory Dictionary, a signature in Estonia is defined as a name written by one's own hand under the text. It emphasizes the uniqueness and individual characteristics of the signer. Finland does not have an official definition of a signature. However, Finnish academic literature describes a signature serving various purposes, including identification, authentication, communication, will, and proof.

When comparing the regulation of digital signatures, Estonia has the Digital Signatures Act, which has been amended multiple times to govern digital signatures. In Estonia, digital signatures have the same legal consequences as handwritten signatures. Finland initially regulated electronic signatures through the Act on Electronic Signatures, but the current legislation in force is the Act on Strong Electronic Identification and Electronic Trust Services. Electronic signatures in Finland are considered equally binding as handwritten signatures.

As the EU is already working on the next step on the electronic identification, both countries are also working on it, based on the already published proposals. In Finland the government has released a proposal for the Digital Identity act.[147]

Both Estonia and Finland have well-established electronic identity systems in place. Estonia has implemented its electronic identity system, known as e-Estonia, with the national ID card (eID

[145] *Digital signing with Finnish ID-cards - ID.ee*. (2021, April 22). ID.ee. Retrieved March 6, 2023, from https://www.id.ee/en/article/digital-signing-with-finnish-id-cards/
[146] *Ibid.*
[147] Hallituksen esitys HE 133/2022 vp Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi

card) playing a central role. The eID card is widely adopted and used for various digital services. Similarly, Finland also has its own electronic identity system that enables secure identification and authentication for electronic transactions and services.

Regarding the types of electronic identity available, Estonia issues various identity documents such as the identity card, residence permit card, digital identity card, and e-resident's digital identity card. Additionally, Estonia utilizes other electronic identification methods, including Mobile ID, Bank ID, Smart ID, username and password, PIN-calculator, and social media accounts. In Finland, electronic identity involves storing certain properties or data about a person in electronic form, including identifying information such as social security numbers or biometric features. Bank IDs are accepted as a means of authentication for private and public services. However, there is no mandatory identity document requirement in Finland.

Both Estonia and Finland comply with the General Data Protection Regulation (GDPR). Estonia has enacted the Personal Data Protection Act (DPA) as a supplement to the GDPR, which sets out general principles and requirements for processing personal data in electronic identity contexts. Similarly, Finland adheres to the GDPR and has the Finnish Data Protection Act (DPA) as additional legislation specific to the country.

Estonia has a notified eID scheme under the eIDAS Regulation, which means that its electronic identification system is recognized and accepted across the European Union. On the other hand, Finland currently does not have a notified eID scheme under the eIDAS Regulation. However, Finland has its own electronic identification system that operates within the country.

The Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity aims to introduce a new European Digital Identity framework. This proposal would have implications for both Estonia and Finland as it seeks to establish a common framework for electronic identity across the EU. The exact impact on the existing regulations and systems of Estonia and Finland will depend on the final version of the regulation and its implementation.

It's important to note that while Estonia is often recognized as a leader in digital governance and electronic services, Finland also has well-developed digital infrastructure and initiatives promoting digitalization. Both countries place importance on electronic identity systems, data protection, and

compliance with EU regulations. Their respective frameworks facilitate secure electronic transactions and protect personal data, ensuring user privacy and fostering trust in digital interactions.

In conclusion, Estonia and Finland have developed comprehensive legal frameworks to safeguard personal data in electronic identity contexts. While there are differences in terms of obligatory identity documents, types of electronic identity available, and specific regulations governing digital signatures, both countries prioritize data protection and compliance with GDPR regulations.

CONCLUSION

This bachelor thesis aimed to conduct a comparative analysis of data protection provisions for electronic identity in Estonia and Finland, with a focus on ensuring compliance and safeguarding user privacy. Through an examination of relevant laws, regulations, guidelines, and scholarly literature, here are some insights into the legal frameworks surrounding electronic identity and data protection in both countries.

When comparing the data protection provisions in Estonia and Finland, it becomes evident that Estonia's Personal Data Protection Act encompasses more comprehensive and stringent provisions specifically related to electronic identity when compared to Finland's Personal Data Act. Estonia's legal framework offers stronger safeguards and measures for protecting individuals' personal data in the context of electronic identity and has a higher protection on electronic signatures than Finland.

Both Estonia and Finland have made significant efforts to align their data protection provisions with the requirements and principles of the GDPR. This alignment demonstrates a commitment to ensuring compliance with EU data protection standards in both countries. The legal frameworks in Estonia and Finland reflect the importance of respecting individuals' rights and safeguarding their personal data.

The implications of these data protection provisions extend to electronic identity systems. The legal frameworks in Estonia and Finland play a crucial role in shaping the design, implementation, and operation of these systems. They address important aspects such as consent requirements, security measures, and user rights, thereby influencing the functionality, security, and user privacy of electronic identity systems in both countries.

By having robust data protection provisions and aligning with the GDPR, Estonia and Finland are taking significant steps to establish a solid legal foundation for the protection of personal data, particularly in the context of electronic identity. These efforts contribute to fostering trust,

enhancing user privacy, and ensuring compliance with EU data protection standards in the digital landscape of both countries.

One contribution of this study is to recommend followingly. Both Estonia and Finland should prioritize continuous review and improvement of their data protection laws to keep pace with technological advancements and evolving threats. Regular updates would ensure that the legal frameworks remain effective in addressing emerging challenges and protecting individuals' personal data. To strengthen the security of electronic identity systems, authorities in both countries should emphasize the implementation of robust security measures. This includes promoting encryption, secure authentication protocols, and putting in place adequate safeguards against data breaches or unauthorized access.

User education and awareness play a crucial role in promoting data protection and electronic identity. Efforts should be made to enhance user education through public awareness campaigns, training programs, and user-friendly resources. Empowering individuals with knowledge enable them to make informed decisions and exercise their rights effectively.

Collaboration and harmonization are key for Estonia and Finland in the context of data protection and electronic identity. Both countries should continue to collaborate at the national and EU levels to promote the harmonization of data protection provisions and electronic identity frameworks. Sharing best practices, exchanging knowledge, and fostering interoperability would contribute to a more seamless and secure digital environment.

By prioritizing continuous improvement, strengthening security measures, promoting user education, and fostering collaboration, Estonia and Finland can ensure the ongoing effectiveness of their data protection laws and electronic identity systems. This would contribute to a safer and more trustworthy digital landscape for individuals and businesses alike.

It is important to acknowledge the limitations of this study. The research focused specifically on the legal aspects of data protection and electronic identity in Estonia and Finland, with a comparative analysis of their respective legislation. Further research is warranted to explore the practical implementation of these legal frameworks, the effectiveness of enforcement mechanisms, and the user experiences with electronic identity systems in both countries.

Future research could also investigate the impact of the proposed European Digital Identity framework and its potential harmonization with the existing national legislation. Additionally, empirical studies could be conducted to gather quantitative and qualitative data on individuals' perceptions, attitudes, and experiences related to electronic identity and data protection in Estonia and Finland.

In conclusion, this study contributes to the understanding of data protection provisions and electronic identity frameworks in Estonia and Finland. The findings highlight the strengths and areas for improvement in the legal frameworks, and the recommendations put forth aim to enhance the protection of personal data and promote secure electronic identity practices. By ensuring compliance with the GDPR and fostering user trust, Estonia and Finland can further advance their digital ecosystems and create a foundation for secure and privacy-respecting electronic identity systems.

The contributions of this work open some research avenues in the field of electronic identity and data protection. The comparison of electronic identity frameworks in Estonia and Finland provides insights into their respective approaches, highlighting the importance of data protection regulations and the role of blockchain technology. The proposed European Digital Identity framework introduces new possibilities for harmonizing electronic identity systems within the EU, while ensuring data protection and privacy. The examination of the Estonian and Finnish regulations, as well as their notified eID schemes, sheds light on the advancements and best practices in these countries, making them valuable case studies for both Finland and Estonia, as well as other nations. Further research can explore the implementation and impact of the proposed regulation, as well as assess the potential benefits and challenges of integrating blockchain technology into electronic identity systems.

LIST OF REFERENCES

Books

1. Bwalya, K. J., & Mutula, S. M. (2014). *E-Government: Implementation, Adoption and Synthesis in Developing Countries*. Walter de Gruyter GmbH & Co KG.
2. Keman, H. (2010). Structure of Government. In M. Sekiguchi (Ed.), *Government and Politics - Volume I* (pp. 159–195). EOLSS Publishers Co. Ltd. https://books.google.ee/books?id=Gkm5DAAAQBAJ&pg=PR1&lr=&hl=et&source=gbs_selected_pages&cad=2#v=onepage&q&f=false
3. Morgan, D., & Parsovs, A. (2017). Using the Estonian Electronic Identity Card for Authentication to a Machine. In *Lecture Notes in Computer Science*. Springer Science+Business Media. https://doi.org/10.1007/978-3-319-70290-2_11
4. Pöysti, T. (1999). Sähköinen identiteetti. In *Encyclopædia Iuridica Fennica: Vol. VII* (pp. 1112–1116). Suomalainen Lakimiesyhdistys.
5. Sharma, S. (2019). *Data Privacy and GDPR Handbook*. John Wiley & Sons.
6. Tsap, V., Lips, S., & Draheim, D. (2020). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In *Springer eBooks* (pp. 159–173). Springer Nature. https://doi.org/10.1007/978-3-030-58957-8_12
7. Voutilainen, T. (2009). *ICT-oikeus sähköisessä hallinnossa : ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely*[PhD dissertation]. Helsingin yliopisto.
8. Windley, P. J. (2005). *Digital Identity: Unmasking Identity Management Architecture (IMA)*. "O'Reilly Media, Inc."

Articles

1. De Andrade, N. N. G. (2013). Electronic identity for europe: Moving from problems to solutions. *Journal of International Commercial Law and Technology*, *8*(2), 104–

109. https://heinonline.org/HOL/Page?handle=hein.journals/jcolate8&id=104&collection=journals&index=

2. Determann, L. (2021). Electronic Form Over Substance: eSignature Laws Need Upgrades. *Hastings Law Journal*, *72*(5), 1385–1452. https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/en/covidwho-1282929
3. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., & Van Eecke, P. (2003b). The legal and market aspects of electronic signatures. *Datenschutz Und Datensicherheit*, *28*(3), 141–146. https://lirias.kuleuven.be/handle/123456789/94918
4. Felt, S., Pappel, I., & Pappel, I. (2016). An Overview of Digital Signing and the Influencing Factors in Estonian Local Governments. *Lecture Notes in Computer Science*, *10018*. https://doi.org/10.1007/978-3-319-48057-2_26
5. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/ijmr-2017-050
6. Ke, T. T., & Sudhir, K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*. https://doi.org/10.1287/mnsc.2022.4614
7. Kelm, S. (2005). On the implementation of the 1999 European Directive on electronic signatures. *Digital Evidence and Electronic Signature Law Review*, *2*, 7–15. https://heinonline.org/HOL/Page?handle=hein.journals/digiteeslr2&id=7&collection=journals&index=
8. Kubicek, H., & Noack, T. (2010). Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. *Identity in the Information Society*, *3*(1), 235–245. https://doi.org/10.1007/s12394-010-0063-x
9. Kutyłowski, M., & Błaśkiewicz, P. (2022). Advanced Electronic Signatures and eIDAS – Analysis of the Concept. *Computer Standards & Interfaces*, *83*, 103644. https://doi.org/10.1016/j.csi.2022.103644
10. Lentner, G. M., & Parycek, P. (2016). Electronic identity (eID) and electronic signature (eSig) for eGovernment services – a comparative legal study. *Transforming Government: People, Process and Policy*, *10*(1), 8–25. https://doi.org/10.1108/tg-11-2013-0047

11. 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*. https://doi.org/10.1007/s10796-022-10363-5
12. López, L. I., Sejersen, T. B., Oakeshott, N., Fajth, G., Khilji, T., & Panta, N. (2012). Civil registration, human rights, and social protection in Asia and the Pacific. *Asia-Pacific Population Journal*, *29*(1), 75–97. https://doi.org/10.18356/ba046677-en
13. Manby, B. (2021). The Sustainable Development Goals and 'legal identity for all': 'First, do no harm.' *World Development*, *139*, 105343. https://doi.org/10.1016/j.worlddev.2020.105343
14. Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, *3*(1), 213–233. https://doi.org/10.1007/s12394-010-0044-0
15. Park, C., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746–1761. https://doi.org/10.1109/tifs.2019.2948287
16. Saarenpää, A. (2003). A Legal Framework for e-Government. *Lecture Notes in Computer Science*, 377–384. https://doi.org/10.1007/10929179_69
17. Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, *12*(24), 12679. https://doi.org/10.3390/app122412679
18. Siems, M. M. (2002). The EU Directive on Electronic Signatures--A Worldwide Model or a Fruitless Attempt to Regulate the Future? *International Review of Law, Computers & Technology*, *16*(1), 7–22. https://doi.org/10.1080/13600860220136075
19. Sperfeldt, C. (2021). Legal identity in the sustainable development agenda: actors, perspectives and trends in an emerging field of research. *The International Journal of Human Rights*, *26*(2), 217–238. https://doi.org/10.1080/13642987.2021.1913409

20. Sullivan, C. (2012). Digital identity and mistake. *International Journal of Law and Information Technology*, *20*(3), 223–241. https://doi.org/10.1093/ijlit/eas015
21. Zwass, V. (2006). The web-internet compound as the infrastructure of digital government. *Business Process Management Journal*, *12*(1), 7–12. https://doi.org/10.1108/14637150610643715

Estonian legislation

1. Digital Signatures Act RT I 2000, 26, 150
2. Electronic Communications Act RT I 2004, 87, 593
3. Identity Documents Act RT I 1999, 25, 365
4. Personal Data Protection Act RT I, 04.01.2019, 11
5. Public Information Act RT I 2000, 92, 597
6. The Health Services Organization Act RT I 2001, 50, 284

EU and international legislation

1. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION 2012/C 326/02 (CFR)
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
3. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)

4. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final (Proposal for eIDAS 2.0 (COM/2021/281 final))
5. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR) 2016/67)
6. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement
7. The European Parliament and the Council of the European Union, Directive 1999/93/EC on a community framework for electronic signatures, 1999
8. The European Parliament and the Council of the European Union, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014 (eIDAS)
9. UN General Assembly. (1948). Universal declaration of human rights (217 [III] A). Paris.

Other countries' legislation

1. Laki sähköisitä allekirjoituksista 14/2003
2. Laki sähköisen viestinnän palveluista 7.11.2014/917
3. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009

4. Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621
5. Laki yksityisyyden suojasta työelämässä 13.8.2004/759
6. Tietosuojalaki (1050/2018)

Other sources

1. Dumortier, J., Kelm, S., Nilsson, H., Skouma, G., & Van Eecke, P. (2003a). *The legal and market aspects of electronic signatures* (C 28.400). Interdisciplinary centre for Law & Information Technology. Retrieved March 31, 2023, from https://www.skilriki.is/media/skjol/electronic_sig_report.pdf
2. *Digital signing with Finnish ID-cards - ID.ee*. (2021, April 22). ID.ee. Retrieved March 6, 2023, from https://www.id.ee/en/article/digital-signing-with-finnish-id-cards/
3. The General Secretariat of the Council. (2022, November 15). *A digital future for Europe*. The Official Website of the Council of the EU and the European Council. Retrieved April 23, 2023, from https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/
4. *Edilex Legal Information Service*. (n.d.). EDILEX. Retrieved April 8, 2023, from https://www.edilex.fi/tietoa_palvelusta/english
5. *eIDAS Terms of Reference*. (n.d.). eIDAS Expert Group (E03032). https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAddtitionalInfo/42178/download
6. *Electronic Identity eID | RIA*. (n.d.). Retrieved March 22, 2023, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/electronic-identity-eid
7. *Estonia - eID User Community* -. (2018, November 7). Retrieved April 28, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Estonia

8. *European Digital Identity*. (n.d.). European Commission. Retrieved October 10, 2022, from https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
9. Hallituksen esitys HE 133/2022 vp Hallituksen esitys eduskunnalle digitaalista henkilöllisyyttä koskevaksi lainsäädännöksi
10. *Overview of pre-notified and notified eID schemes under eIDAS - eID User Community -*. (2019, September 13). Retrieved May 1, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS
11. Saarmets, V. (2011). (Üld)tuntud ja tundmatu (ema)keel 2. In *Ajakiri Õiguskeel*. Estonian Ministry of Justice. Retrieved March 6, 2023, from https://www.just.ee/media/339/download
12. *Tallinn University of Technology Library portal Primo*. (n.d.). Tallinn University of Technology Library Portal Primo. Retrieved February 4, 2023, from https://tutl-primo.hosted.exlibrisgroup.com/primo-explore/search?vid=372TUTL_VU1&sortby=rank&lang=en_US
13. *The European Digital Identity Wallet Architecture and Reference Framework*. (2023, February 10). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
14. The General Secretariat of the Council. (2022, November 15). *A digital future for Europe*. The Official Website of the Council of the EU and the European Council. Retrieved April 23, 2023, from https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/
15. *What is the legislation - esignature*. (n.d.). Retrieved March 3, 2023, from https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/What+is+the+legislation+-+esignature

Appendix 4. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[1148]

I Asa Kawamura (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis, The European Union Electronic Identity And Data Protection In The Finnish And Estonian Legal Systems

(*title of the graduation thesis*)

supervised by Maria Claudia Solarte Vasquez, LLM, PhD,
(*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

11.5.2023
_____ (date)

[148] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*