https://doi.org/10.22364/jull.12.02

Electronic Signature Under the eIDAS Regulation in Domestic and Cross-Border Communication: Estonian Example

Dr. iur. **Irene Kull***
Faculty of Law, University of Tartu
Professor of Civil Law
E-mail: *irene.kull@ut.ee*

Laura Kask
Faculty of Law, University of Tartu
PhD Student
E-mail: *kasklaura1@gmail.com*

The aim of the article is to analyse issue of cross-border recognition and harmonized rules of electronic signatures under the eIDAS Regulation, which is intended to enable cross border electronic transactions. The authors reveal whether the legal order of the Estonia reflects the changes that have occurred in the field of electronic signatures since eIDAS Regulation. This article examines the legal consequences of a new distinction between the levels of electronic signature in the legal order of a Member State in private transactions and administrative procedures and the conditions under which cross-border recognition of electronic signatures in the European Union takes place.

Keywords: digital single market, eIDAS Regulation, electronic signature.

Contents

* The research led to this article was financed by Estonian Research Council grant PUT PRG 124.

Introduction

A Digital Single Market is the realm where the free movement of goods, persons, services and capital is ensured and where individuals and businesses can smoothly access and exercise online activities in a fair competition and high level of consumer and personal data protection, irrespective of their nationality or place of residence[1]. The realization of the four fundamental freedoms of the European Union also requires the free movement of data. In an electronic environment, people and services are not transferred, but information is. In order to ensure reliable cross-border communication, it is necessary to identify, by whom and under which conditions the transactions have been made and the contracts concluded. As the digital environment does not recognize national borders and transactions increasingly take place across borders, an interoperable electronic environment is important for the competitiveness of the European Union.

The debate about whether the identification of individuals in the digital environment should be a norm and an obligation, or should the digital environment be a form of expression of our privacy and anonymity, has not disappeared to this day. Although it can be argued that anonymity is an essential part of a democratic cultural concept[2], the author's assessment should not, however, be oblivious to the fact that in creating a credible digital environment, individuals need to know who with and on what basis they make transactions. This, however, does not restrict the person's freedom to remain anonymous.

The electronic signature that is equal to handwritten signature helps to save time equal to one working week in a year for each working-age adult,[3] giving time and resources and an appreciable competitive advantage for developed e-states. The ability to identify yourself securely via the internet via an ID card or other e-identity tool or to provide an electronic signature is also available in other EU Member

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. 06.05.2015, COM(2015) 192 final. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN [last viewed 30.11.2018].

[2] *Turk, K.* Digitaalkeskkonnas isiku tuvastamise meetmete poolt ja vastu [Pros and Cons of the Measures Used for Identifying Persons in the Digital Environment]. *Juridica*, No. 3, 2014, p. 176.

[3] E-Estonia overview. See more at: https://estonia.ee/overview/ [last viewed 30.11.2018].

States (e.g. Latvia, Austria, Finland, Belgium, Spain), but the main means of communication for cross-border services is paper.[4]

Even though in 1999 Directive 1999/93 / EC of the European Parliament and of the Council on a framework for electronic signatures providing for the mutual recognition of signatures[5] was adopted, electronic cross-border communication in the European Union is still not widely used. This is mainly due to the uneven implementation of the e-signature directive in the Member States, the different technological levels of the countries, the lack of technical interoperability solutions, as well as cultural differences.[6] eIDAS Regulation of 2014[7] is the next attempt to take cross-border transactions to electronic channels and support the uptake of electronic signatures.

The aim of the article is to analyse the issue of cross-border recognition and harmonized rules of electronic signatures under the eIDAS Regulation**,** which is intended to enable cross border electronic transactions. As the monopoly of service providers in the field has shifted and the mutual recognition of service providers would mean the consumer has a wider choice of picking the service being used, the national legal orders have to cope with the challenges created by the new levels of electronic signatures. The authors explore, whether the legal order of the Estonia reflects the changes that have occurred in the field of electronic signatures since eIDAS Regulation and how the differentiation of the levels of electronic signatures affect the legislative framework in place. As the legal framework should reflect the practices in place, it is analysed if the Estonian private law needs to be amended or there is no practical challenge and the need might emerge from the court practice. The article does not address the electronic authentication and liability of the service provider and service user.

1. Concept of Signature and Formal Requirements of Contracts

In order to analyse the legal meaning of electronic signature and its regulation on national and EU level, it is necessary to agree on the meaning of terms used. Signature can be defined as a handwritten depiction of someone's name, nickname, or even a simple 'X' or other mark that a person writes on documents as a proof of identity and intent.[8] Oxford English Dictionary defines signature as a person's name written in a distinctive way as a form of identification in authorizing a cheque or

[4] *Varik, H.* E-identiteet Eesti ja Euroopa Liidu õigusruumis: Euroopa Parlamendi ja Nõukogu e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määruse kohaldamine Eestis – kujunemislugu, probleemid ja eelseisvad väljakutsed [E-Identity in the legal area of Estonia and the European Union: application of the Regulation of Trust Services necessary for e-Identity and e-transactions of the European Parliament and the Council in Estonia – the history of development, problems and impending challenges]. Master thesis. Tallinn, 2015, p. 4.

[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *OJ*, L 013, 19.01.2000, pp. 12–20.

[6] According to id.ee, there are 1 267 547 active ID-cards and the population of Estonia is 1,311,800. See more: https://www.stat.ee/ee. Estonian internet users are at the forefront of internet use in Europe in areas like online banking (91%) and the consumption of news content (91%). See more at: https://ec.europa.eu/digital-single-market/en/scoreboard/estonia [last viewed 30.11.2018].

[7] 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. *OJ*, L 257, 28.08.2014, pp. 73–114.

[8] The definition from Wikipedia. See more about the meaning of signature at: https://en.wikipedia.org/wiki/Signature [last viewed 30.11.2018].

document or concluding a letter.[9] DCFR defines person's signature as handwritten signature, electronic signature or advanced electronic signature, and anything being signed by a person (art. I.-1:107(1)) to follow the non-discriminatory approach to any type of signature used in practice for authentication. Estonian legal system does not have legal definition of the concept of 'signature'.[10] What is more, EU law does not provide definition of a signature while all aspects related to the requirements regarding documents are outside of the scope of harmonization purposes.[11] Estonian Explanatory Dictionary defines 'signature' as a handwritten name, which is tied to a text,[12] giving the notion that a signature is something that identifies the person and the text on which it can be found.

While considering the function of written signatures, it is important to distinguish between the concepts of a 'written form' and of a 'handwritten signature'. DCFR art. I.-1:107(2) explains 'handwritten signature' as the name of, or sign representing, a person written by that person's own hand for the purpose of authentication and writing as textual form, on paper or another durable medium an in directly legible characters.[13] Under Estonian law, the written form means a document which contains a hand-written signature of a person entering the transaction unless otherwise provided by law (§ 78(1) GPCCA[14]). Mechanical signature is also deemed to be equal to handwritten signature, only if mechanical signature is in common usage and the other party does not require a hand-written signature at once (§ 78(2) GPCCA). It has to be mentioned that if the contract has to be in written form, written declarations of intention arising from the contract may be communicated also by other means which allow written reproduction of the declarations of intention (§ 78(3) GPCCA).

Estonia adapted electronic signature as formal requirement of electronic form in 01.07.2002,[15] although Digital Signatures Act[16] entered into force already in 2000, setting the formal technical requirements of an electronic signature, but the first digital signature was issued on October 7, 2002.[17] Before eIDAS Regulation, the legal framework consisted of Digital Signatures Act and GPCCA. According to

[9] Oxford English Living Dictionary. Available: https://en.oxforddictionaries.com/definition/signature [last viewed 30.11.2018].

[10] For example, US Uniform Commercial Code defines (§ 1–201(37)) signed as 'using any symbol executed or adopted with present intention to adopt or accept a writing. Writing' includes printing, typewriting, or any other intentional reduction to tangible form'.

[11] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, art. 1. *OJ*, L 13, 19.01.2000, pp. 12–20.

[12] Eesti keele seletav sõnaraamat [Estonian Explanatory Dictionary]. Available: http://www.eki.ee/dict/ekss/index.cgi?Q=allkiri&F=M [last viewed 24.03.2019].

[13] For more information see DCFR Annex. Definitions. Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). *C. von Bar, E. Clive, H. Schulte-Nölke* (eds.). Sellier, European Law Publishers, 2009. Available: https://sakig.pl/uploads/upfiles/moot/dfcr.pdf [last viewed 30.11.2018].

[14] General Part of the Civil Code Act (GPCCA), in force from 01.07.2002. Available in English: https://www.riigiteataja.ee/en/eli/509012018002/consolide [last viewed 30.11.2018].

[15] The requirements were formulated under the harmonisation with the rules of the directive 1999/93/EU and directive 2000/31/EU (directive on electronic commerce).

[16] Digital Signatures Act, in force from 15.12.2000. Available: https://www.riigiteataja.ee/en/eli/ee/508072014007/consolide [last viewed 30.11.2018].

[17] The first contract where digital signature was used was between the mayors of Tallinn (Edgar Savisaar) and Tartu (Andrus Ansip) who signed a Memorandum of Understanding to tighten the cooperation between the cities in the sphere of IT. For more information see: https://sk.ee/uudised/taitub-aasta-eesti-esimesest-digitaalallkirjast (available in Estonian) [last viewed 30.11.2018].

§ 80 of GPCCA, in order to comply with the requirements for the electronic form, a transaction shall be entered into in a form enabling repeated reproduction, contain the names of the persons entering into the transaction and be electronically signed by the persons entering into the transaction. An electronic signature, also digital signature, shall be given in a manner which allows the signature to be associated with the content of the transaction, the person entering into the transaction and the time of entry into the transaction. The procedure for attributing an electronic signature to a person and for giving electronic signatures shall be provided by law (§ 80 GPCCA). So, digital signatures will primarily be used to prove the identity of a person and higher level of security and are considered to have the same legal consequences as handwritten signatures.

Although the uptake of electronic signatures was not as quick as it was expected, the 10th year of digital signatures celebrated the magical number of 100 million signatures given and it took less than 3 years to achieve 200 million.[18] Today more than 99.6% of banking transactions are done online and 99.3% of people declare taxes online.[19] This means the electronic channels and electronic signatures have become a commodity in Estonia, although the recent vulnerability case[20] and security incidents across the world might explain the fear that still exists in legal certainty in comparison to handwritten signatures. What is more, the existing legal regulation still tends to be based on handwritten signatures and paper documents. Therefore, the possibility of a security breach or data leakage might hold back the broader acceptance of electronic signature as the main mean of authorizing transactions in national and cross-border usage.

Although there is no legal definition of a signature, the definition could be taken from the grammatical interpretation and legislator has made the connection between the signature and a person wanting to enter into a transaction in order to prove the will. Electronic signature is legally defined and a certain type of electronic signature is equal to handwritten signature, giving the parties of the transactions and third parties a valid ground to understand the will and the essence of the transaction.

---

[18] For more information and statistics see: https://www.id.ee/?lang=en&id= [last viewed 30.11.2018].

[19] E-Estonian fact sheet. Available: https://e-estonia.com/wp-content/uploads/updated-facts-estonia.pdf [last viewed 30.11.2018].

[20] On the evening of 30 August, 2017, a researcher with the Centre for Research on Cryptography and Security at Masaryk University notified Estonia of a security vulnerability (so-called ROCA vulnerability) on the chips used in the Estonian ID card. Over a billion chips were impacted globally, among them those used on Estonian ID cards issued since autumn 2014. Theoretically, the security vulnerability could have allowed the private key (which is used for authentication and signing) to be calculated from the public key – in theory, making it possible to clone the victim's cryptographic keys and use them for authentication, sign or decrypt documents even without being in physical possession of the card. For more information see: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf [last viewed 30.11.2018]. See more about the ROCA vulnerability: ROCA vulnerability and eID: Lessons learned. Information System Authority. Estonian Republic. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf [last viewed 30.11.2018].

2. Usage of Electronic Signatures in Estonia Before eIDAS Regulation

Estonian private law is based on the principle of freedom of form, declared in the § 77(1) GPCCA and § 11(1) of the Law of Obligations Act (LOA)[21]. The § 77(1) GPCCA provides general rule that a transaction may be entered into in any format unless a mandatory format of the transaction is provided by law, § 11(1) LOA specifies that the contract may be entered into orally, in writing or in any other form if there are no other required forms provided by law. All requirements concerning different forms are described in the GPCCA.[22]

Every formal requirement has to have a reasonable purpose. For example, handwritten signature is intended to fulfil following functions: to make clear that parties came to the consensus and are intended to be bound by the contract, to warn the parties that by signature they are entering into a binding transaction or to provide an evident in case of dispute.[23] Electronic signature performs the same functions as handwritten signature since it is not an independent formal requirement, but an option that replaces the requirement of signature written by hand. However, electronic signature is equal to a transaction in written form only as long as it allows the signature to be associated with the content of the transaction, the person entering into the transaction and the time of entry into the transaction (§ 80(3) GPCCA).

Before eIDAS Regulation, there was only one kind of electronic signature, defined as 'digital signature', which was equal to handwritten signature and regulated by law, namely, Digital Signature Act. The term 'electronic signature' was used in Estonian legal doctrine as general term, e.g., it did not encompass only digital signature.[24] Nevertheless, there are other possibilities to sign a contract electronically. An example can be drawn with receiving a parcel post, where the acceptance of the parcel is usually done using a stylus. A person is handed a machine where the signature is given with a pencil called stylus and it will create the image of a handwritten signature. However, technically and legally it is not an equivalent of a handwritten signature. There is also a possibility to sign documents by using a fingerprint or an eye retina. Using those methods can be qualified as signing electronically. According to MIT Technology Review, paying with your face, e.g. authorizing transaction with face recognition is among 10 breaktrough technologies in 2017.[25] The previous and new technologies can be considered as electronic signatures but until they are given the legal validity of electronic signature equal to handwritten signature, they are only considered as a signature in electronic form. As far as law does not provide any mandatory requirements concerning the form of the transaction or signature, the parties can agree on any

---

[21] Law of Obligations Act (LOA), in force from 01.07.2002. Available: https://www.riigiteataja.ee/en/eli/508082018001/consolide [last viewed 30.11.2018].

[22] Estonian GPCCA provides following kind of formal requirements: written form (§ 78), form which can be reproduced in writing (§ 79), electronic form (§ 80), notarial certification of transaction (§ 81), notarial authentication of transaction (§ 82).

[23] Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne [General Part of Civil Code Act. Commented edition]. *P. Varul, I. Kull, V. Kõve, M. Käerdi* (eds.). Tallinn: Juura, 2010, p. 243.

[24] General Part of Civil Code Act. Commented edition (note 22), p. 259. About the use of digital signature before eIDAS Regulation in Internet voting see *Madise, Ü., Vinkel, P.* Constitutionality of Remote Internet Voting: The Estonian Perspective. *Juridica International*, No. 18, 2011, pp. 3–16.

[25] *Knight, W.* Paying with your face. MIT Technology Review. Available: https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face/ [last viewed 30.11.2018].

kind of electronic signature, which satisfies their needs and provides required security in respective legal relations.

EIDAS Regulation entered into force in 01.07.2016. An electronic signature remains defined by art. 3(10) of eIDAS Regulation as "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign". However, there has not been the differentiation of electronic signatures or the concept of levels of electronic signatures in Estonian legal framework. As the functionality of an ID card encompasses the possibility to sign and the signature is technically and legally equal to handwritten signature, there has not been a market of service providers offering different types of electronic signatures. The main problem concerning conclusion of contracts electronically in Estonia might be that the legal framework for accepting anything else than the electronic signature equal to handwritten signature, has been too strict. For example, if the law provides that contract has to be concluded in the form which can be reproduced in writing (§ 79 GPCCA), the only possibility to sign it electronically has been a digital signature, which corresponds to the qualified e-signature in the eIDAS Regulation.[26] Digital signature has also been the only possible signature to conclude the contract in electronic form under the § 80 GPCCA.

In conclusion, Estonian legal system has not differentiated the levels of electronic signatures until July 2016 when the eIDAS regulation became into force. The term used for electronic signature equal to handwritten signature has been 'digital signature' and the term 'qualified electronic signature' is unknown to citizens, but also lawyers and others operating in Estonia and abroad. Nevertheless, it can be stated that the term 'digital signature' can only be used in case of an electronic signature that meets the requirements of a qualified e-signature in the eIDAS Regulation.

3. Electronic Signatures in Estonia Since eIDAS Regulation

In order to ensure that the usage of the different levels of electronic signatures regulated under eIDAS Regulation in public and private transactions, the national law must reflect the change of paradigm and facilitate the distinguishing of the levels of electronic signatures.[27] The existing Estonian regulation imposes conflicts with the eIDAS regulation, as the participants in private relations have too strict requirements, since in order to comply with the electronic form requirements, the electronic signature that is equal to handwritten signature is needed. This means that no lower level signature can be used, although the aims of the signature and electronic form can also be met with lower levels of signature.

In Estonia, the Police and Border Guard Board issues identity documents, and from 2002 the electronic document is issued in addition to the physical document. Identity Document Act[28] § 9(5) states that the information which enables identification of a person digitally, including a cryptographic key enabling digital identification and the respective certificate, and information which enables digital signing, including a cryptographic key enabling digital signing and the respective

[26] eIDAS Regulation, art. 3(12).

[27] See more in *Dumortier, J.* Regulation (EU) No. 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). Available at SSRN: https://ssrn.com/abstract=2855484 [last viewed 30.11.2018].

[28] Identity Document Act, in force from 01.01.2000. Available: https://www.riigiteataja.ee/en/eli/526042018001/consolide [last viewed 30.11.2018].

certificate, and other digital data may be entered in a document. The functionality of an ID-card allows electronic authentication, gives an opportunity to express declaration of intention by signing documents electronically and allows to encrypt and decrypt the files.

As mentioned before, since the eIDAS Regulation was enforced, the Estonian legislators had to make a choice whether to change the long-rooted term 'digital signature' and transpose the terminology being used in the eIDAS Regulation. The change would have resulted in changing almost all the acts that include interactions with the state, procedural acts, etc. Therefore, the legislator decided to continue to use the terms already employed in legal acts. According to Electronic Identification and Trust Services for Electronic Transactions Act, a digital signature shall be deemed an electronic signature that conforms to the requirements for a qualified electronic signature set out in article 3(12) of eIDAS Regulation.[29] Consequently, whenever the Estonian legislation uses the term 'digital signature', it means the qualified e-signature.

According to the eIDAS Regulation, a qualified e-signature is an equivalent of a handwritten signature (article 25(2)). This is a general principle, which makes cross-border recognition of signatures legally possible. However, the Member States of the European Union have a margin of discretion in deciding, on the basis of a transaction or proceeding, the formal nature of the electronic transaction in a particular situation. Hence, although in a Member State, under a transaction law, an e-signature can also be signed, it may not be possible in a similar transaction in another Member State, as the legislation requires an electronic signature equivalent to a handwritten signature. Therefore, in spite of the directly applicable regulation, the legislator will decide which of the transactions or procedures and which formality requirements apply.

Although the main service used for electronic signing in Estonia is signing with the state-issued electronic document emitted on the basis of Identity Documents Act, there has been an increase in private sector service usage. It is important for the person to understand the level of the particular e-signature and in which processes and transactions its use is legally and technically possible. The existing Estonian regulation imposes conflicts with the eIDAS regulation, as the participants in private relations have overly strict requirements – in order to comply with the electronic form requirements, the electronic signature that is equal to handwritten signature is needed. The freedom of form gives the parties the ability to agree on a transaction with different levels of electronic signatures, but if there is the electronic form requirement, only electronic signatures that are equal to handwritten signatures can be used. Since, according to the eIDAS Regulation, e-signatures that are in line with the Regulation should be in free circulation in the internal market, Member States have an obligation to support the use of solutions by different service providers.

[29] Electronic Identification and Trust Services for Electronic Transactions Act, in force from 12.10.2016. Available: https://www.riigiteataja.ee/en/eli/527102016001/consolide [last viewed 30.11.2018].

4. Regulation of Digital Signature in European Union

4.1. Historical Introduction

On 16 April 1997, the Commission presented to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions a Communication on a European Initiative in Electronic Commerce.[30] The development of digital signatures was mentioned as one of the elements in building trust and confidence among businesses and consumers in use of digital technology. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signature was adapted on 19.01.2000 to promote interoperability of electronic-signature products, to facilitate the use of electronic signatures and to contribute to their legal recognition.[31]

Since the e-signature directive did not achieve the desired objective, the European Council recommended in its 4 February and 23 October 2011 conclusions that the European Commission should for 2015 set up an integrated digital single market in key areas for the digital economy to facilitate the cross-border use of Internet-based services.[32] The considerations of European Commission included the factor that a direct regulation would improve the situation. eIDAS regulation should aim to boost the trust in services in the internal market for e-identity and electronic transactions and is a legal instrument designed to support confidence in electronic transactions in the internal market. The biggest goal of the regulation is to support the foundations of the Digital Single Market. EIDAS Regulation establishes a common basis for secure electronic communication between citizens, businesses and public authorities and increases the efficiency of public-private internet-based services in the European Union.[33] The regulation should make it easier to use cross-border e-services and help create the same level of trust towards the digital environment as opposed to the physical world, since it sets out common principles for the recognition of electronic identities and e-signatures by European public authorities.

Although the eIDAS Regulation does not cover the procedural rules in national legal order, the legal framework of electronic signatures should be unified across the European Union in order to meet the aims of Digital Single Market Strategy and the eIDAS Regulation. eIDAS Regulation is directly applicable in all 28 EU member states without need of being transposed into local laws. It will replace the overwhelming part of all national signature laws associated to the 1999 Directive. Nevertheless, eIDAS Regulation still leaves areas that can be regulated under domestic law[34] and the implementation of the eIDAS Regulation depends on national regulation adopting the framework. In Estonia the act implementing the eIDAS Regulation is Electronic Identification and Trust Services for Electronic

[30] Electronic Commerce: Commission presents framework for future action. Available: http://europa.eu/rapid/press-release_IP-97-313_en.htm?locale=en [last viewed 30.11.2018].

[31] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *OJ*, L 13, 19.01.2000, pp. 12–20, art. 1(1).

[32] eIDAS Regulation, recital 4.

[33] eIDAS Regulation, recital 2.

[34] In that sense the eIDAS Regulation can be compared to 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). *OJ*, L 119, 04.05.2016, pp. 1–88.

Transactions Act in force from 26.10.2018.[35] With the entry into force thereof, the Digital Signature Act has become invalid and the new legislative framework consists of eIDAS Regulation and its implementing acts, Electronic Identification and Trust Services for Electronic Transactions Act and its implementing acts.

4.2. Levels of Electronic Signatures in eIDAS Regulation

The eIDAS Regulation sets various levels of e-signatures, and e-signature is a general term that covers the various levels of e-signature provided for by the regulation. In accordance with article 3(10) of the eIDAS Regulation, e-signature means electronic data that is attached to, or logically linked to other electronic data and used by the signing authority for the purpose of signing. The eIDAS Regulation distinguishes four levels of e-signatures, which are (1) a qualified e-signature, (2) an advanced e-signature, issued with a qualified certificate, (3) an advanced e-signature, and (4) another e-signature, which does not meet the requirements of the eIDAS Regulation. The Regulation is designed to be tech-neutral and the aim is to support new technologies.

The highest level of e-signature is a qualified e-signature under article 3(12) of the eIDAS Regulation, which is an advanced e-signature, which is provided by a qualified e-signature creation device, based on an e-signature qualified certificate. In order to meet the requirements of the qualified e-signature, the following three conditions must be met: First, the signature must meet the requirements of advanced e-signature. The requirements for advanced e-signature are in accordance with article 26 of the eIDAS Regulation are the following: the e-signature is uniquely linked to the signatory, it is capable of identifying the signatory, it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control and it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. Secondly, a qualified electronic signature device must be used when signing. For example, the signature chip must be certified in accordance with article 30 of the eIDAS Regulation. Thirdly, the signature must be based on an e-signature qualified certificate, that is, comply with the requirements of article 28 of the eIDAS Regulation.

The next level of e-signature is an advanced e-signature, that uses a qualified certificate but the difference between the qualified e-signature and advanced e-signature is that the signature creation device is not certified. Other than that, the advanced e-signature meets the same requirements as a qualified e-signature, giving the guarantee that it is possible to identify the relationship between a signed document and a signatory.

The lowest level signature is an advanced e-signature, an e-signature that must comply only with the terms of article 26 of the eIDAS Regulation which means either the certificate nor the device is qualified (has passed a certain audit and meets the certification standards).

An electronic signature that does not meet any of the requirements of the eIDAS Regulation is a so-called other e-signature, which, however, is still permitted in some transactions.

With the entry into fore of eIDAS Regulation, the definitions of e-signatures have become part of Estonian legal system and there is no definition in national

[35] Available in English: https://www.riigiteataja.ee/en/eli/527102016001/consolide [last viewed 30.11.2018].

law. In Estonian private law, there is the freedom of form and the compulsory requirements for a contract to be valid on the basis of the signature used are only in very specific areas. It's up to the organization to define the level of evidential weight they want to rely on if a document is signed electronically. They may opt to apply e-signatures on a lowest level or can demand the highest level possible which is considered equal to handwritten signature. However, the evidential value of an electronic signature is usually higher and can be controlled more easily than the usage of handwritten signature and the considerations of using the advanced e-signature with a qualified certificate is certainly fulfilling the aims the signature orgininally has. It depends on the risk-assessment and the level of acceptance in the private sector organization, which e-signature is accepted and can be differentiated on the basis of the consequences the transaction is bringing.

4.3. Cross-Border Recognition of E-signatures in European Union

Cross-border recognition of signatures is not really a new obligation. The obligation was also laid down in the e-signature directive, which was transposed into Estonian law in accordance with § 40 of the Digital Signatures Act, which provided that certificates issued by a foreign certification service provider were recognized as equivalent to the certificates issued by the certification service provider operating in Estonia. At least one of the conditions set out in § 40 of the Digital Signatures Act had to be fulfilled in order to recognise the signature. This still meant that only e-signatures that were meeting the same standards as the digital signatures (qualified e-signatures) were considered equivalent.

According to the eIDAS Regulation, Member States are required to treat all signatures of the same level equally. The legal effects it grants should be achievable by any technical means provided that the requirements of the eIDAS Regulation are met.[36] As article 25(3) of the eIDAS Regulation stipulates that a qualified electronic signature based on a qualified certificate issued in one Member State shall be recognized as a qualified electronic signature in all other Member States. Article 27 of the eIDAS Regulation states that if a Member State requires an advanced electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognized advanced electronic signatures, advanced electronic signatures based on a qualified certificate for electronic signatures, and qualified electronic signatures in at least the formats or using methods defined in the implementing acts meaning that the Estonian public sector is required to accept documents signed using other service providers' solutions that meet the level of e-signature that is allowed to use by national legislation. The Regulation does not enforce private sector to accept the e-signatures from other member states, although the framework and common standards are set and compulsory acceptance by public sector should encourage private sector to follow.

According to article 22(1) of the eIDAS Regulation, each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them. The Estonian Trusted List is kept by Estonian Technical Regulatory Authority, who also acts as a trust service supervision authority (§ 2(3) Electronic Identification and Trust Services for Electronic Transactions Act). The trusted lists of the Member States

[36] eIDAS Regulation, recital 27.

are combined into European Union Trust List,[37] which provides information about who are the qualified service providers operating in the internal market and what services they provide.[38] Electronic signing is one of the trusted services.

A trusted list has, however, been created for the communication between the computers and allow software to distinguish between applications that are used by the service (whether qualified or not). Implementing acts have been created for the implementation of the eIDAS Regulation, of which the Implementing Act of e-signatures[39] clearly refers to the standards of the European Telecommunications Standards Institute (ETSI). The e-signatures that are created according the standard, must be accepted and should be understood by the Member States.

However, it must now be acknowledged that the legal framework is in place for the recognition of e-signatures, but the development of technical solutions to address all the different levels of e-signatures that are in use in the European Union is still ongoing at the European Commission and at the national level. In Estonia, the State Information Authority is responsible for developing solutions, which plans to create technical solutions that would allow validation of e-signatures.[40]

Therefore, cross-border recognition of e-signatures is not only a legal obligation, but there is a need to raise awareness that e-signature capabilities that are used in national processes are equally applicable to cross-border communication. In order to understand the level of the e-signature the legal framework is of little use and does not give answers that would be useful for people and businesses using the different levels of e-signatures. It is necessary to create technical solutions to help individuals make informed decisions and understand the legal validity of a document signed by a person using an e-signature service provided by an unknown service provider.

4.4. Cross-Border Recognition of E-signatures Outside European Union

Although the digital environment is not country-specific, the regulation on mutual recognition of e-signatures will only apply to the European Union (and the economic area). If, in the past, the possibility for such reciprocal recognition was regulated in accordance with national law and bilateral agreement between the states, then from the entry into force of the eIDAS Regulation, trust services provided by trusted service providers established in a third country in accordance with article 14(1) shall be recognised as legally equivalent to qualified trust services

[37] EU Trusted List. Available in XML format: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml [last viewed 30.11.2018]. See more about EU Truste List: https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers [last viewed 30.11.2018].

[38] The procedure to be listed in a trusted list is a long procedure and for the purpose and scope of this article it is not analysed further.

[39] Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to articles 27(5) and 37(5) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, article 27(5) and 37(5). *OJ*, L 235, 09.09.2015, pp 37–41. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D1506&from=ET [last viewed 30.11.2018].

[40] Different government officials in State Information Authority have discussed the plans about creating the solutions but up to 01.11.2018 no working solution is yet created for public use. *Reimo, T.* Allkirjatasemetest rakendustes [Signature levels in applications]. Available in Estonian: https://www.ria.ee/sites/default/files/content-editors/usaldusteenused/usaldusteenused2017-tonis_reimo_1.pdf [last viewed 30.11.2018].

provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with article 218 TFEU. Thus, for example, it is not possible for Estonia and Georgia to agree on the mutual recognition of e-signatures by a bilateral agreement, but only if the European Union and Georgia would have the relevant agreement. The recognition of third-country e-signatures is likely to require, first of all, the functioning and cooperation of e-signatures on EU level, and then it will be possible to open the single market to e-signatures of countries outside the European Union.

5. Levels of E-signatures Used in Practice: Estonian Example

5.1. Examples of Qualified Electronic Signatures

5.1.1. ID card

The digital signature, i.e. ID card or other documents issued on the basis of the Identity Documents Act (e-residency, digital identity etc), is equivalent to a handwritten signature, as it meets all the requirements for qualified e-signatures, including the qualified signature creation device (i.e. a chip). The electronic functionality of the document can only be used with a special chip reader and have a special software downloaded to your computer.

5.1.2. Mobile ID

An electronic authentication and electronic signature can also be done and given with Mobile ID, the certificate for digital identification and the digital signature is issued pursuant to § 20^4(1) of the Identity Documents Act, and the certificates are associated with a mobile phone SIM card. Using Mobile ID requires a SIM card that supports this solution. The SIM is issued by the telecom operators (Elisa, Tele2, Elion). The chip used for signing with Mobile ID is the qualified signature creation device. This means electronic signature given with Mobile ID is a qualified e-signature and is equal to handwritten signature as it complies with all the requirements for a qualified e-signature in eIDAS Regulation.

5.1.3. Smart ID

At the beginning of 2017, Smart ID was launched in Estonia and other Baltic states, which was founded by SK ID Solutions AS and Cybernetica AS. For Smart ID, authentication and electronic signing is created inside the smart gadget (that needs to be connected with WIFI) so that it is easy to use on a smartphone or tablet, without the need for accessories such as a dedicated SIM card or card reader. [41] The need for the new authentication means supports the implementation timeframe for PSD2 directive,[42] which sets clear rules for electronic authentication of the bank customers. Smart ID in Estonia was planned to replace parole-cards and other lower level authentication means and create extra layer of security for authorizing transactions. Therefore, it is mostly used in banking systems. Since 8 November

[41] Smart ID. Available: https://sk.ee/en/services/smart-id [last viewed 30.11.2018].

[42] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC. *OJ*, L 337, 23.12.2015, pp. 35–127.

2018 Smart ID is also considered as qualified e-signature creation device meaning the e-signature given with it is equal to handwritten signature.

5.2. Examples of Non-Qualified Electronic Signatures

5.2.1. Smart ID

Nevertheless, there is still a period between which the e-signatures created by Smart ID were not considered equal to handwritten signatures. After the entry into force of the eIDAS Regulation, each e-signature creation device must undergo a certification process that was not required by service providers before the eIDAS Regulation. This is a procedurally relatively complex process in which the compliance of the service provider with the requirements set out in the regulation (article 24 eIDAS Regulation) and the corresponding audit are checked. In addition, the audit findings (art. 20(1) eIDAS Regulation) must be submitted to the Supervisory Authority every 24 months, at the time of compliance with both the eIDAS Regulation and the relevant standards and the certification of the e-signature instrument (art. 30 eIDAS Regulation). In case of Smart ID, the certification process was finished by November 2018, which means the e-signatures given up to this date or with the certificate that is not renewed, are considered one level lower. In the terms of eIDAS Regulation this is an advanced e-signature with a qualified certificate, but it is not equal to handwritten signature. The signature given to Smart ID will become equivalent to a self-signed signature only after a qualified trust service has undergone a conformity assessment and the service has been entered in the Trusted List. All of the e-signatures that have been given before are advanced e-signatures that are issued using a qualified certificate. This means there is a more complex practice and the situation where only qualified e-signatures that are equal to handwritten signatures has changed.

5.2.2. Stylus

One of the possibilities to sign the document is to use touch-sensitive pen or stylus. In that case the signature is given as handwritten signature. Stylus is defined as a computer accessory that is used to assist in navigating or providing more precision when using touchscreens. The most known is the use of stylus upon receipt of parcels. Signature given on the screen by using stylus is similar to a person's signature, the question arises whether this could be treated as handwritten signature equal to the signature on the paper.

In addition to parcel delivery, the image of the signature is used on a driver's license and identity card being an additional security measure that allows for a better checking of identity. In such cases, a signature is issued in the presence of an official or employee who verifies that the signature is provided by the person whose personal data is entered on the document. The signature image given to the screen and then to the document allows the other persons to compare this signature with the signature later on by the person in other cases. The driver's license and identity card also have a person's facial image and date of birth, which is also helpful in checking identity. However, a stylus signature image can be affixed to any document without the person and document having any identifiable link. That is why the signature given on the screen pen cannot be considered equivalent to a self-signed signature. However, this type of signature is appropriate in operations where an electronic signature that is equivalent to a handwritten signature is not required.

6. Obligation of Service Provider to Provide Information About the Level of E-signature

Although the eIDAS Regulation does not affect national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules, customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means.[43] It is the duty of the service provider to provide information about the service being offered and art. 13(2) of eIDAS Regulation states that when trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations. The limitations should be taken into account with the national rules on liability.

According to Estonian LOA § 48(1)5) a trader shall provide the consumer prior to entry into a contract or making a binding offer by a consumer for this purpose, in the case of digital content, the method of use thereof, the technical protective measures applied to it and compatibility thereof with any hardware and software of which the trader is aware or should be aware. The level of the e-signature is definitely something the person who would like to use the service needs to be aware of. LOA (§ 15(2)) states that if, upon entry into a contract, one party is or should be aware of circumstances which do not constitute a violation of formalities but render the contract void or if such circumstances are caused by the party, the party shall compensate the other party for the damage created due to the fact that the other party believed the contract to be valid.

Smart ID is a service where there is the possibility to create two different levels of e-signatures – advanced e-signature with qualified certificate (from the launch of the service to 07.11.2018 and with the certificates not being renewed) and qualified e-signature with qualified certificate and qualified signature creation device (since 08.11.2018). The terms and conditions of Smart ID describe the level in the terms used by eIDAS Regulation,[44] but the information is definitely not sufficient for the consumer to enable a person who is not a professional in the field to understand the difference between qualified and non-qualified e-signature. What is more, Estonian legislation uses the term 'digital signature' and the common understanding in the society is that there is only one level of electronic signature and it is equal to handwritten signature. There has not been any court practice yet, but it would be debatable if the service provider is meeting the information requirements and what would be the consequences if the contract is signed using the wrong form of e-signature. Therefore, it would be advisable for the service provider to specify the terms and conditions.

In order to sign the documents with the state- issued electronic certificates (ID card) or with the state-supported electronic certificates (Mobile ID), you need to download a special software. Estonian Information System Authority is responsible

[43] eIDAS Regulation. Recital 37.

[44] Terms and Conditions for Use of Certificates of Certificates (for qualified Smart ID and non-qualified (advanced) Smart ID). Available: https://www.sk.ee/en/repository/conditions-for-use-of-certificates/ [last viewed 30.11.2018].

for the functioning, development, and management of ID software (the DigiDoc application) designated for the end user.[45] The software allows to get information about the signed documents and the signatory (person, time, role, validity, etc.). The software gives information whether the e-signature is valid or invalid ('green' or 'red'), including whether it is an equivalent to handwritten signature. It also provides information whether there are any limitations for the usage. For example, if a non-qualified Smart ID is used for a transaction, users are warned that it is an e-signature that can be used for operations that do not require a qualified e-signature or electronic signature equivalent to handwritten signature. However, the software cannot assess all the e-signatures that are used across the EU, and therefore the service providers need to take the responsibility to inform the service users. Nevertheless, the information provided at the moment should redirect users to alternative solutions for identifying the e-signature level and help them to make a more informed decision in accepting or sending the documents being signed electronically.

The differences in technical level and the interoperability across the EU would take time for eIDAS Regulation to be fully implemented. Although forward-looking states like Estonia are offering software that can assess the level of the e-signature without the need of the user to understand the trusted list or the technical nuances behind the different terms and levels of e-signatures. As the eIDAS Regulation is not interfering into the national law in terms of the requirements of information and liability clauses, national law is setting the obligation of the service provider to enclose the details about the service which includes the level of e-signature in a way it would be understandable for a person without expert knowledge. Today the service providers tend to use the terminology of eIDAS Regulation that is not revealing the information about the service.

7. Usage of Electronic Signatures in Private Transactions

eIDAS Regulation is not regulating the usage of electronic signatures in private transactions, leaving the national legislation to govern the formal requirements and consequences transactions not meeting the formal requirements. Despite the fact that prior to the entry into force of the eIDAS Regulation, the different levels of signatures in Estonia were not described, the legislator has found that a digital signature is just one form of electronic signature (§ 80(3) GPCCA), which has also left the possibility to use other e- signatures. Consequently, GPCCA supports the general principles of the eIDAS Regulation, according to which the electronic signature is a general term, and it is possible to take into account the differentiation of levels for the determination of a particular transaction.

However, there is some controversy between § 78 and § 80 of the GPCCA because, although it is possible to use lower-level e-signatures in the case of an electronic form, in order to fulfil the written formal requirement, the document must be signed only with a handwritten signature, which in electronic channel would mean with a qualified e-signature (e.g. ID card, Mobile ID, Smart ID since 08.11.2018). Therefore, it could be considered that in the case of a lower-level e-signature (e.g. Smart ID until 7.11.2018), the requirement for a written reproduction form are fulfilled, in which, according to § 79 of the GPCCA, the

[45] For more information see: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html [last viewed 30.11.2018].

transaction must be made in a permanent way in a manner allowing the written retransmission and include the names of the persons who made the transaction, but do not need to be signed with a signature equal to handwritten signature.

If there is no special requirement in the law, the transaction may be signed with any level e-signature in order to comply with the requirements of the format capable of reproducing the written reproduction. In the case of a lower-level e-signature, it is necessary to eliminate the contradiction of § 78(1) and § 80(1) of the GPCCA, which should remain the responsibility of the legislator or the case law, in order to comply with the electronic formality requirement for completeness. Based on the comments GPCCA and the definitions of the eIDAS Regulation, the lower-level signature should also comply with the requirements of the electronic format, but the grammatical interpretation of § 78 of the GPCCA does not allow it. If a law or agreement requires a handwritten signature or an equivalent electronic signature, it may only be replaced by a qualified electronic signature also meaning a digital signature in Estonian legislation.

In private transactions, failure to comply with the formal requirements set out in law or agreed upon by the parties generally leads to the transaction considered void. The failure to comply with the formal requirement of a transaction being concluded by handwritten signature or the equivalent electronic signature by signing the transaction with a lower level of e-signature is a non-compliance with a formal requirement. However, when deciding on the consequences, the purpose of the formal requirement, the actual will of the parties and the principle of good faith must be taken into account. When using an e-signature of a level different from the agreement of the parties, it is important to take into account the purpose of the formality of the agreement in order to determine the actual will of the parties to decide if the transaction could be deemed void. It would also be important to interpret the behaviour of a person and whether the duties agreed on the basis of the transaction have been executed.

Summary

Over 650 million digital signatures have been given in Estonia by March 2019. Today, the usage of digital signatures has become a daily routine for the private sector as well as the public sector. Equalizing the processes of the analogue world and the digital environment has laid the foundation for the emergence of an e-state. As a digital single market is a priority of the European Union, the eIDAS Regulation is an important backbone supporting the cross-border usage of online services. The aim of the eIDAS Regulation is to boost trust and convenience in secure and seamless cross-border electronic transactions.

The implementation of the new Regulation is challenging within the Estonian legal framework, as it sets levels for e-signatures which have been unknown in Estonian legislation. It is important to distinguish between the legal consequences of the usage of e-signatures so that individuals could make a conscious and legally binding decision in transactions.

Before eIDAS Regulation the electronic signatures used in Estonia could have been split conditionally into two: digital signatures and other electronic signatures. The eIDAS Regulation sets different levels of signatures and term 'electronic signature' is a general term. It is important to distinguish between the legal consequences of the distinction between the levels of electronic signature so

that individuals can make a conscious and legally binding decision in transactions, taking into account the formal requirements of the transaction. In Estonian private law, the freedom of form is established as a general principle, with the right to stipulate formal requirements applicable to transactions by law or by agreement of the parties. Therefore, if there is no special requirement in the law, the transaction may be signed with any level of e-signature in order to comply with at least the requirements for a format capable of reproduction in writing. However, if a law or agreement requires a handwritten signature or an equivalent electronic signature, it may only be replaced by a qualified electronic signature or digital signature. However, the authors are of the opinion it would be necessary to amend the law or leave the court practice to decide, whether the lower-level e-signature complies with the requirements of the electronic form. The grammatical interpretation of § 78 and § 80 of the GPCCA is not supporting the opinion.

Since the level of e-signature has not been differentiated in Estonian legislation before the entry into force of the eIDAS Regulation, and there is no case law on this issue, the authors consider that if the requirement for a handwritten signature or equivalent electronic form is non-compliant, the court should take into account the current practice and the intention of the parties, the purpose of the formal requirement, the actual will of the parties and the principle of good faith. The authors are not supporting the amendment of law and distinguishing the e-signature levels in private transactions. When an e-signature used is different from the agreement of the parties, it is important to take into account the purpose of the formal agreement in order to determine the actual will of the parties.

In addition to the national legal order, the eIDAS Regulation introduces changes in cross-border communication. Although states can support the uptake by developing software and helping the interoperability, there is the obligation of the service providers to give information about the service, including the level of e-signature. Recognition of cross-border e-signatures is not only subject to a legal obligation, but there is a need to raise awareness, provide correct information and create technological solutions so that electronic means that are in use in national processes can also be used equally in cross-border communication.

Sources

Bibliography

1. *Bar, C. von, Clive, E., Schulte-Nölke, H.* (eds.). Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). Munich: Sellier, 2009.
2. *Dumortier, J.* Regulation (EU) No. 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). Available at SSRN: https://ssrn.com/abstract=2855484 [last viewed 30.11.2018].
3. *Erlich, M.* E-allkirjad Euroopas ja nende käsitlemine Eestis. Juhend ja nõuanded e-allkirjade käsitlemiseks [E-Signatures in Europe and their treatment in Estonia. Guide and tips for handling e-signatures]. Riigi Infosüsteemi Amet, 2016.
4. *Knight, W.* Paying with your face. MIT Technology Review. Available: https://www.technologyreview.com/s/603494/10-breakthrough-technologies-2017-paying-with-your-face [last viewed 30.11.2018].
5. *Madise, Ü., Vinkel, P.* Constitutionality of Remote Internet Voting: The Estonian Perspective. *Juridica International*, No. 18, 2011.
6. Oxford English Living Dictionary. Available: https://en.oxforddictionaries.com/definition/ [last viewed 30.11.2018].
7. Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). *C. von Bar, E. Clive, H. Schulte-Nölke* (eds.). Sellier, European Law Publishers, 2009. Available: https://sakig.pl/uploads/upfiles/moot/dfcr.pdf [last viewed 30.11.2018].

8. *Reimo, T.* Allkirjatasemetest rakendustes [Signature levels in applications]. Available in Estonian: https://www.ria.ee/sites/default/files/content-editors/usaldusteenused/usaldusteenused2017-tonis_reimo_1.pdfArvutivõrgus [last viewed 30.11.2018].
9. Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaanne [General Part of Civil Code Act. Commented edition]. *P. Varul, I. Kull, V. Kõve, M. Käerdi* (eds.). Tallinn: Juura, 2010.
10. *Turk, K.* Digitaalkeskkonnas isiku tuvastamise meetmete poolt ja vastu [Pros and Cons of the Measures Used for Identifying Persons in the Digital Environment]. *Juridica*, No. 3, 2014.
11. *Varik, H.* E-identiteet Eesti ja Euroopa Liidu õigusruumis: Euroopa Parlamendi ja Nõukogu e-identimise ja etehingute jaoks vajalike usaldusteenuste määruse kohaldamine Eestis – kujunemislugu, probleemid ja eelseisvad väljakutsed. Magistritöö [E-Identity in the legal area of Estonia and the European Union: application of the Regulation of Trust Services necessary for e-Identity and e-transactions of the European Parliament and the Council in Estonia – the history of development, problems and impending challenges]. Master thesis. Tallinn 2015.

Normative Acts

1. Digital Signatures Act, in force from 15.12.2000. Available: https://www.riigiteataja.ee/en/eli/ee/508072014007/consolide [last viewed 30.11.2018].
2. General Part of the Civil Code Act (GPCCA), in force from 01.07.2002. Available in English: https://www.riigiteataja.ee/en/eli/509012018002/consolide [last viewed 30.11.2018].
3. Electronic Identification and Trust Services for Electronic Transactions Act, in force from 12.10.2016. Available: https://www.riigiteataja.ee/en/eli/527102016001/consolide [last viewed 30.11.2018].
4. Identity Document Act, in force from 01.01.2000. Available: https://www.riigiteataja.ee/en/eli/526042018001/consolide [last viewed 30.11.2018].
5. Law of Obligations Act (LOA), in force from 01.07.2002. Available: https://www.riigiteataja.ee/en/eli/508082018001/consolide [last viewed 30.11.2018].
6. 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. *OJ*, L 257, 28.08.2014, pp. 73–114.
7. 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). *OJ*, L 119, 04.05.2016, pp. 1–88.
8. Trust Services for Electronic Transactions Act in force from 26.10.2018. Available: https://www.riigiteataja.ee/en/eli/527102016001/consolide [last viewed 30.11.2018].

Other Sources

1. Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to articles 27(5) and 37(5) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *OJ*, L 235/37, 09.09.2015.
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. 06.05.2015, COM(2015) 192 final.
3. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *OJ*, L 013, 19.01.2000, pp. 12–20.
4. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC. *OJ*, L 337, 23.12.2015, pp. 35–127.
5. Electronic Commerce: Commission presents framework for future action. Available: http://europa.eu/rapid/press-release_IP-97-313_en.htm?locale=en [last viewed 30.11.2018].
6. EU Trusted List. Available in XML format: https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml [last viewed 30.11.2018].
7. Smart ID. Available: https://sk.ee/en/services/smart-id [last viewed 30.11.2018].
8. Terms and Conditions for Use of Certificates. Available: https://www.sk.ee/en/repository/conditions-for-use-of-certificates/ [last viewed 30.11.2018].

Abbreviations

Art.	Article
DCFR	Draft Common Frame of Reference
GPCCA	General Part of Civil Code Act (Estonia)
eIDAS Regulation	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
EU	European Union
ID Card	identification card
LOA	Law of Obligations Act (Estonia)
No.	Number
Para.	Paragraph
ROCA vulnerability	Return of Coppersmith's Attack vulnerability
US	United States of America