https://doi.org/10.12697/JI.2024.33.05

Laura Kask

CEO, Proud Engineers
Doctoral student, University of Tartu

Time of Signing:

Legal Requirements and Technical Options for Hand-written and Electronic Signatures[*1]

Abstract. The article examines the legal and technical aspects of determining the time of signing for both hand-written and electronic signatures. Of particular relevance in light of the widespread utilisation of electronic signatures in Estonia, involving both government-issued and private-sector e-signatures, it explores how signatures are linked to the time of transactions and whether the time of signing affects the validity of signatures under Estonian and European Union law. The paper discusses the general principle of freedom of form in transactions, highlighting the formal requirements imposed by law for certain transactions and wills, with special focus on comparing the traditional analogue world with the digital environment. Additionally, a review of recent amendments to the eIDAS Regulation examines their impact on the union's electronic-signature ecosystem. Discussion addresses technical challenges also, with specific regard to linking a signature to the time of the transaction and the legal implications of timestamping in the domain of electronic signatures. For broader context, the insight is informed by comparison with Norway, another member of the European Economic Area. The research reported upon contributes to awareness of the importance of understanding both the legislative framework and technical practices involved in identifying the time of signing for ensuring the legal validity and reliability of electronic signatures.

Keywords: eIDAS Regulation, electronic signatures, time of signing, validity of electronic signatures

1. Introduction to the landscape

The principal e-signature[*2] instrument used in Estonia is a document (a physical ID card, digital ID, 'mobile ID', e-residency card, or residence-permit card) issued by the Police and Border Guard Board on the basis of the Identity Documents Act[*3] (hereinafter, 'IDA'). This document is utilised in conjunction with an electronic document with a digital identification certificate and a digital-signature certificate (discussed below). In

1 This paper has been written as part of the project 'Societal Security and Digital Identities' (project number 320785) financed by the Norwegian Research Council.

2 According to the eIDAS Regulation, art 3(22), an e-signature device is a piece of appropriately configured software or hardware that would be used for e-signing.

3 Or *Isikut tõendavate dokumentide seadus*: RT I 1999, 25, 365; RT I, 26.4.2024, 13.

addition to government-issued e-signatures, private-sector e-signatures are witnessing increased use (with Smart-ID signatures being a key example).[*4] On 7 October 2002, the mayors of Tallinn and Tartu digitally signed an inter-city co-operation agreement, thus establishing the first digitally signed document, and in a 20-year span since then, more than 800 million signatures have been provided via Estonia's ID-card, Mobile-ID, and Smart-ID systems.[*5] Given that Estonia has a population of 1.3 million, these volumes attest that handling the exchange of declarations of intent and the conclusion of contracts electronically has become commonplace in the country, where it permeates the public and private sector both.

Notwithstanding the well-established general principle of freedom of form[*6], transactions exist for which a mandatory form requirement is imposed by law. Mandatory formal requirements for transactions and wills may be provided for also by specific agreement. A signature might be required for statements of intent in cases of analogue or electronic transactions, and the variety of actions that are considered to represent intent has grown wider as new technical solutions become available.

The article compares signing and the determination of the time of signing between the analogue world and the electronic environment to answer the question of how it is possible to link a signature to the time of the transaction. The examination here identifies an answer to whether the time of signing has a legal effect on the validity of the signature and, hence, is required by Estonian and European Union (EU) laws. Further discussion considers some examples, mainly from Norway, which is closely associated with the EU through its membership in the European Economic Area. For a well-grounded answer to the questions probed, the paper describes the technical set-up for e-signing, thereby clarifying which time expressed in the e-signature software has legal meaning and should be regarded as the e-signature time. Because there are technological challenges, the paper analyses the recent amendments made at EU level (mainly with regard to the eIDAS Regulation[*7] and its amendments[*8]) and on Estonian level additionally, alongside how they affect the ecosystem of electronic signatures.

The legislative framework and technical practice connected with the time of signing are especially deserving of analysis since the recent amendments to the eIDAS Regulation are going to influence the ecosystems in all EU countries and there have not been many scientific articles in this field (of particular relevance is technical research into the theoretical possibility of changing the registered time of signing[*9] after the electronic signature is issued). By examining these matters and the larger constellation of related issues, the article contributes also to research in such areas as electronic identification (eID) and trust services in domestic and cross-border transactions. The discussion is based on foundations the author and a colleague laid in an article published in *Juridica* in 2020[*10].

4 Smart-ID, a service provided by SK ID Solutions AS, has been recognised nationally as a qualified e-signature tool since November 2018. An electronic-identification service, it uses an application on a person's phone (itself called Smart-ID) and the Smart-ID system's key-management-server service. Smart-ID credentials can be issued to those persons with an Estonian personal identification code. An expert group appointed by the Information System Authority (RIA) found the assurance level for electronic identification issued to persons with an Estonian personal identification code to be 'high' with Smart-ID. Further details are provided on the Smart-ID Web site <https://www.smart-id.com/et/smart-id/> accessed on 28 February 2024.

5 In 20 years, more than 800 million digital signatures have been produced in Estonia, according to the country's Information System Authority <https://www.ria.ee/en/news/20-years-more-800-million-digital-signatures-have-been-given-estonia> accessed on 28 February 2024.

6 General Part of the Civil Code Act (*Tsiviilseadustiku üldosa seadus*), s 77(3); see RT I 2002, 35, 216; RT I, 6.7.2023, 98.

7 Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on e-identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257, 28.8.2014, 73.

8 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *OJ L2024/1183, 30.4.2024*.

9 Further information is available: T Mets and A Paršovs, 'Time of Signing in the Estonian Digital Signature Scheme' (2019) 16 Digital Evidence and Electronic Signature Law Review 40. – DOI: https://doi.org/10.14296/deeslr.v16i0.5076. The author continues closely examining the research and analysing how new amendments to the legislative framework could settle the technical possibility.

10 L Kask and K Laanest, 'Elektroonilise allkirjastamise aja tuvastamine: õiguslikud nõuded ja tehnilised võimalused [Determining the Time of Electronic Signing: Legal Requirements and Technological Possibilities]' (2020) 4 Juridica 294 <https://www.id.ee/wp-content/uploads/2022/10/j_20_4_294.pdf> accessed on 29 March 2024.

2. Time of signature of the declaration of intent and the transaction

2.1. Time of signing in the case of hand-written signatures

A declaration of intention makes the will of a person visible to the/each other party and legally binding; i.e., it expresses the will to entail certain legal consequences. A transaction is an act or a set of interrelated acts within the meaning of Section 67 (1) of the General Part of the Civil Code Act (GPCCA) that includes a declaration of intent to produce a specific legal effect. The statement of intention could be called the core of the transaction, without which no transaction can be concluded.[*11] A transaction may encompass several statements of intent, made by several persons. In particular, an expression of intention might be articulated via such an action as concluding a last will and testament, submitting a draft contract, executing withdrawal from a contract, or proposing modification to a contract[*12]. Statements of intent must be made by an identifiable person, and therefore written statements of intent are signed irrespective of whether a written form is required for either the contract or the statement of intent. Also, a signature is among the forms of expressing the completion of a statement of intent, which results in the transaction being deemed to have been carried out or contributed to by a specific person. That person must understand what they have agreed to, what they have signed, and what consequences follow from their intention.

Section 77 (1) of the GPCCA establishes the freedom of form of transactions, together with the right to prescribe by law or by mutual agreement of the parties the formal requirements applicable to transactions.[*13] Notwithstanding the principle of freedom of form, it is necessary to take account of certain subsequent problems, related to proving the substance of the transaction in the course of judicial proceedings.[*14] Although Estonian law at present does not define the form for a transaction, the form is the external expression of the transaction. The main functions of the requirements imposed as to the form of a transaction are to serve a warning function (to avoid undue haste and thoughtless or careless execution of the transaction), an advisory function (in particular where, for example, a notary's services are employed), and a verification function (to facilitate subsequent ascertainment and verification of the fact of the transaction and its substance).[*15] However, the signature constitutes confirmation of the party's will and gives the other party/parties to the contract or third parties additional assurance that said person has expressed their true will. The authors of the commentaries to the GPCCA have acknowledged that a hand-written signature must be placed at the end of the transaction document, to delimit the extent of the content of the transaction, and that the signing must be expressed in such a way as to enable the signatory to be identified. For the signer's identification, the signatory need not write their full name, nor does evidence that they have made a mistake in producing the signature (e.g., omitting a letter) necessarily preclude identification of the person signing. A signature that is illegible but written in such a way that it can be attributed without doubt to a specific person may be sufficient.[*16] The signature provides information that the making of a declaration of intent has reached its final stage – i.e., that the parties have reached an agreement or that the person in question has become convinced that a transaction is taking place – and that this is being expressed via a signature sufficiently personal to allow the declaration of intent to be attributed to a specific person.

Section 78 provides that, where the law specifies written form for the transaction, the transaction document must be signed in writing by the parties to that transaction. Although the written-form requirement is characterised by hand-signing, the law does not define signature by hand, nor does it mandate that the hand-signing and the legal effect be linked to the time of signature or specify details for this. The intention that is to be confirmed must be identified on a case-by-case basis.[*17] There are, however, special provisions by dint of which it is important that the hand-written document indicate the day and year if it is to comply

11 P Varul, 'Tahteavaldus ja selle tegemine [Declarations of Intention]' (2010) 7 Juridica 497.

12 Ibid.

13 P Varul and others (eds), *General Part of the Civil Code Act, Commented Edition* (Juura 2010) 243.

14 K Sein, 'Tehingu vorminõuded ja nende järgimata jätmise tagajärjed [Requirements for the Format of Transactions and Consequences of Failure To Respect Such Requirements]' (2010) 7 Juridica 510.

15 I refer to the requirements imposed with regard to the form of the transaction as described by Sein (ibid 509).

16 *General Part of the Civil Code Act* (n 13) 248.

17 Ibid 249.

with the formal requirement. For example, according to Section 23 (1) of the Law of Succession Act[*18], a will prepared in one's home must be written from beginning to end in the testator's own hand, indicate the date (including the year) of execution, and be signed by the testator. The same rule applies under Section 42 of the Norwegian Inheritance Act[*19], where it is stated that a will drafted in the home must be in writing, the testator must sign the document, and it shall be dated. In both cases, a last will and testament prepared at one's home cannot be only electronically signed, and there is an explicit aim of the legislator to ensure that the testator and witnesses were physically in the same location at the relevant moment. In the analogue world, in the case of a hand-signed will, the time of signature is important for the expression of the will, particularly where the legal effects of the transaction are linked to a certain period of time. The obligation to indicate the time may also be imposed through an agreement between/among the parties or by their established mutual practice, when the parties consider said agreement/practice to be legally binding.

However, signing the entire document and indicating the time does not in itself necessarily mean that the signature confirms acceptance of all the terms and conditions reflected in the document. For example, the Estonian Supreme Court in civil case no. 3-2-1-144-09[*20] held that the acceptance and/or signature of an invoice does not generally imply that the recipient of the invoice agrees to terms and conditions set out in the invoice that were not agreed upon previously. For the terms indicated in the invoice to become part of the parties' agreement, the invoice should state clearly that its acceptance is intended to encompass agreement to terms not previously accepted. Accordingly, the mere fact of signing a document is insufficient for assessment of the actual intention of the person who signed it. The conduct of that person too must be assessed, as must past practices and customs in activities between/among the parties. The foregoing conclusion is confirmed by the position taken by the Supreme Court with regard to civil case 2-17-14766, according to which the mere fact that a document was signed later rather than at the time stated in the contract (a situation of intellectual forgery) did not exclude the legal consequences arising from the contract.[*21]

It is clear from the above that the law does not define a hand-written signature[*22]; neither does it generally require the time of signature to be specified for transactions. The time of signature is not necessarily decisive with respect to the legal consequences. The Supreme Court has held in its case-law that, as a rule, it is irrelevant in civil law when a document was drawn up and that it having been drawn up later does not preclude the legal consequences from ensuing. There certainly are exceptions, but this description captures the main direction of legal thought.

2.2. Time of signing in an e-signature setting

While in the analogue world the validity of a transaction carried out in writing and authenticated by means of a hand-written signature does not, in general terms, require the time of signature to be linked to the time of the transaction, an electronic form equivalent to a written form imposes additional conditions on the link between the signature and the transaction. According to Section 80 of the GPCCA, electronic form is equivalent to written form.[*23] According to the commentary to the GPCCA, the electronic form is not a separate type of transaction form; it merely is an equivalent that supersedes a written form, unless the law provides otherwise, and its validity requires three conditions to be met.[*24] Firstly, the transaction must be

18 Or 'Pärimisseadus': RT I 2008, 7, 52; RT I, 6.7.2023, 67.

19 Or the Act on Inheritance and Succession of Estates (Inheritance Act) (*Lov om arv og dødsboskifte (arveloven)*) ACT-2019-06-14-21 <https://lovdata.no/dokument/NL/lov/2019-06-14-21/KAPITTEL_2-6-1#%C2%A742> accessed on 28 February 2024.

20 RKTKo 3-2-1-144-09, 17.12.2009 [11].

21 RKTKo 2-17-14766, 9.4.2020 [15]. See also RKTKo 2-16-3785/114, 3.4.2019 [14]; RKTKo 3-2-1-96-13, 23.10.2013 [34].

22 It should be reiterated that this must be written in such a way as to enable the signatory to be identified; therefore, one could argue that three crosses or a single letter is not sufficient for a hand-written signature. Nevertheless, a decree of the Minister of Justice on the list of examinations performed at the Estonian Institute of Forensic Science attests that said institute provides expert opinion on hand-written signatures. Experts resolve identification quandaries related to identification of the signer. See 'Eesti Kohtuekspertiisi Instituudis tehtavate ekspertiiside loetelu [List of Examinations Performed at the Estonian Institute of Forensic Science]' RT I, 8.9.2023, 20; RT I, 7.9.2023, 23 ('Nora Kasemaa ekspertiisibüroo'). A description of the service is available in Estonian at <https://ekspertiisibyroo.ee/et/ekspertiis/kaekirjaekspertiis/> accessed on 29 March 2024.

23 For details, see also CM Laborde, *Electronic Signatures in International Contracts* (Frankfurt am Main, Peter Lang 2010) 2017. – DOI: https://doi.org/10.3726/978-3-653-00124-2.

24 *General Part of the Civil Code Act* (n 13) 250–251.

executed in a form that can be reproduced in a manner allowing for permanent reproducibility; secondly, the medium must include the names of the persons who have entered into the transaction; and, thirdly, there must be electronic signing by those persons (see Section 80 (2) of the GPCCA). Under Section 80 (3) of the GPCCA, an electronic signature must be provided in a manner that allows the signature to be associated with the content of the transaction, the person taking part in that transaction, and the time when the transaction was executed. Therefore, when an electronic signature is used to express an intention, not only the identification of the content of the transaction and the identity of the person, as expressed under the general rule for hand-written signatures, are important; the time of signature too is of relevance.

That said, the legislation does not specify the level of granularity (i.e., the unit of time) or precision to which an electronic signature must be capable of being linked to the time of the transaction such that the condition set is considered to be met. It also does not specify which action[*25] required for an electronic signature is the one that should be linked to the time of the transaction. Neither does the law define the time of the transaction in any other way. But the GPCCA does regulate setting of time limits, which under Section 134 (2) of the GPCCA are stated in numbers of years, months, weeks, days, hours, or smaller time units from the transaction date or by reference to a definite event. This approach could inform determining the time of the transaction also. In the case of an electronic signature, the time of the transaction must be determined in a manner taking into account that the time is given in the signature container to the nearest second. From a legal point of view, it is possible for a due date to be expressed through a time limit calculated in units of time smaller than a day (per Section 136 (10) of the GPCCA), but time limits are not expressed in seconds (or to seconds' granularity) in real-world practice. As for delimiting of days for the purpose of expressing a time limit (per the GPCCA's Section 136 (9)), the relevant span runs from one midnight to the next midnight. Seconds are not relevant here either: expression in hours and minutes indicates whether the relevant statement of intention or document has been filed within the time limit (before '12:00am' or '2400').

Thus the unit of time for determining the time of e-signature can be derived from the law, but the link between the time of e-signature and the time of the transaction is left to practice. Importantly, there is no difference in legal meaning between a hand-written signature and an electronic signature, since, even in an electronic environment, the signing of a document is not sufficient to assess the actual intention of the person who signed it (in that the conduct of the person too must be evaluated, alongside the custom and previous practice established mutually by the parties), since the agreement may be concluded in any manner so long as it is sufficiently clear that the parties have reached an agreement. Signatures used in civil claims differ, depending on the requirements for e-signature. This is discussed in more detail below.

2.3. Making and receiving a signed declaration of intent

If one is to ascertain the meaning of time in the case of an electronic transaction, it is necessary to analyse the rules governing the making and receipt of a signed declaration of intent, since time obtains legal meaning only when the declaration of intent is made and delivered. Since the rules applicable to the declaration of intent do not distinguish between an e-signature and a hand-written signature, the question arises of whether the general rules on the making of a declaration of intent apply to e-signatures.

For execution of a transaction, a declaration of intent is required. According to Section 69 (1) of the GPCCA, a declaration of intent addressed to a specific person must be expressed by the person making the declaration of intent and becomes valid upon receipt. Under its Section 69 (2), a declaration of intention made to an absent person is deemed to have been received and thus become valid when it has reached the addressee's residence or domicile and when the addressee of the declaration of intention has a reasonable opportunity to acquaint themselves with it. The notion of reasonable access refers to the statement of intention having reached the addressee; the burden of knowing its contents rests with the recipient of the statement of intention. In the event of a dispute, the sender of the statement of intent must prove that the statement of intent has entered the 'sphere of influence' of the addressee, except in the case of a notice of breach of contract as provided for in Section 70 of the GPCCA (a notice pertaining to a breach of contract shall be deemed to have been received at the time when it would have been received under normal

[25] For a description of the e-signature process, see 'How To Sign an ID-Card Document in [the] DigiDoc4 Client' <https://www.id.ee/index.php?id=38801> accessed on 28 February 2024. For more information on the steps required to e-sign, see Section 4 of this article.

circumstances if the sender proves that they reasonably expressed their intention). The addressee of the statement of intention, in turn, must prove that they did not receive it if asserting as much.[*26]

If an electronic signature is used, the declaration of intent is sent to the other party electronically. Proving that the declaration has reached its addressee is somewhat easier when an electronic channel rather than a physical channel is used. Nowadays, there is a wide variety of means of transmission available, which in many situations can increase the efficiency of the delivery of information. This is no longer just a matter of sending electronically signed declarations of intent as attachments to email; alternative mechanisms may involve transferring files via third-party 'cloud' platforms (Google Drive, Dropbox, etc.) or social-networking sites (Facebook, WhatsApp, and others). Although the Supreme Court has dealt with the question of when an email message is to be considered received (in civil case 3-2-1-123-07), there is some question as to whether, given the various technical possibilities that have emerged over the years, it is possible to describe the time of receipt in a uniform way across all forms of transmission. The Supreme Court concluded in the case of transmission by email that the email must be deemed to have reached the addressee when it has arrived on the server of the addressee or of the service provider of his or her choice. However, an email message shall be deemed to have been received within the meaning of Section 69 (1) of the GPCCA only when the addressee has a reasonable opportunity to acquaint themselves with it. When the person has a reasonable opportunity to access email or a particular email message with particular formatting, links, scripting, language, etc. depends on the specific circumstances of the case, including whether or not the addressee has a permanent Internet connection. In business and professional activities, a person should be expected to check their email at least once a day. Therefore, in the course of business and professional activities, an email message can be deemed accessible on the day following the day on which it arrived on the server of the recipient or of the recipient's chosen service provider, at the latest.[*27] Though presented in 2007, the position described above is still valid today[*28], irrespective of the fact that the use of the Internet and overall ability to access one's emails have increased and that email typically reaches the final server (the recipient's or service provider's) in a fraction of a second. Therefore, there is no technological justification or any need for revising the position of the Supreme Court according to which a statement of intention sent by email – one of the instruments that fall under the definition connected with an electronic signature – should be deemed to be accessible from the day following the day on which the email is received. Therefore, that position supplies some framing for the meaning of time with regard to when the intention of a party is shown to and accessed by another party.

At the same time, several social-networking applications ('Messenger' services offered by Apple, Facebook, etc.; WhatsApp; and various others) through which documents can be exchanged allow the recipient to see when a message sent to them was first opened. For example, Facebook Messenger shows the time at which each message was read, and WhatsApp indicates whether a file or message has been viewed. While this is standard practice in two-party communication wherein the content of the transaction requires immediate delivery, setting a time for receipt (i.e., a given time at which the message is to reach the recipient's sphere of influence) by agreement is possible for statements of intent sent via innovative technological solutions. For example, with some technological solutions that allow the parties to see the time at which the other person has opened the message and/or that record the time of sending, the parties may link the time of receipt of the expression of intent to the time at which the message is read.[*29] At the same time, activities involving standard contracts must comply with Section 42 (3) (35) of the Law of Obligations Act[*30] (LOA), according to which regulating assessment of the receipt of a statement of intent

26 Varul (n 11) 503.

27 RKTKo 3-2-1-123-07, 21.12.2007 [12]. A somewhat different rule follows from the Draft Common Frame of Reference's art I-1:109(4)(-)(d), according to which a communication sent electronically is deemed to be received if the recipient has access to it – i.e., if email has reached the recipient's server; see also UNCITRAL Model Law on Electronic Commerce 1996, art 15(2); UNIDROIT Principles (Rome 2004) 29.

28 The legislator has introduced exceptions to the general rule that the information must be deemed to have been served. For example, according to s 314^1(1) of the Code of Civil Procedure (RT I 2005, 26, 197; RT I, 19.3.2019, 23), a procedural document sent by means of telecommunication shall be deemed to have been served three working days after its sending.

29 Since 1 January 2013, courts have, in addition, had the right to contact defendants via, for example, Facebook, which should help speed up proceedings. While documents cannot be considered served in these conditions, it is possible to send a notification of service to the Facebook account. For more details, see M Teder, 'Kohtud võivad inimeste leidmiseks ka sotsiaalvõrgustikke kasutada [Courts Can Use Social Networks To Find People]' (*Postimees*, 2 January 2013) <https://www.postimees.ee/1090258/kohtud-voivad-inimeste-leidmiseks-ka-sotsiaalvorgustikke-kasutada> accessed on 29 March 2024.

30 Võlaõigusseadus: RT I 2001, 81, 487; RT I, 8.1.2020, 10.

in a manner different from that provided for by law is unfair and void in the context of standard terms. Obviously, this does not preclude agreeing on a time for making the declaration of intent.*[31]

Although technology makes it possible to find out the time of receipt of the statement of intent and the parties may legitimately agree on the time noted for receipt of the statement, technical capacity and the principle of reasonableness should certainly be considered to dictate the time of receipt of a statement of intent expressed by electronic signature. It may be difficult to read the content of a statement of intent received electronically for reason of a lack of technical capacity. For example, while the validity of an e-signature can be verified by means of specific software, the software involved may be structured somewhat differently from one country to another. In assessment of reasonable opportunity to consult the declaration of intention*[32], factors such as the time needed to set up the technical environment and the person's technical ability to handle such e-signatures must therefore be considered.

It can be concluded, then, that there is no difference in the legal requirements for making and receiving a signed declaration of intent between the analogue world and the electronic domain. In the case of an electronically transmitted statement of intent, the technical mechanisms available provide a wider range of possibilities for verifying the receipt of both signed and unsigned statements of intent.

2.4. Authentication as sufficient means of showing intent in an electronic environment

As more and more transactions get handled via e-services, the differentiation between authentication (using an electronic identity issued by a commercial service provider or by a government) and trust services (using e-signature or e-seal*[33] mechanisms) is gaining importance. A recent study*[34] revealed a strong preference among Nordic countries (expressed the most clearly by Finland, Sweden, Norway, and Denmark) to focus on authentication when considering the cross-border dimension and only after that on electronic signatures. A cross-border web of trust between eID schemes would be the most important element, since more than 90% of residents have means available to them*[35] for accessing e-services while not necessarily possessing an electronic-signature-creation device. In the Nordic–Baltic region*[36] there is a very clear divide: Estonia, Latvia, and Lithuania rely on e-signature for their electronic transactions whereas the other countries have deemed authentication a sufficient means of showing one's intent online. While reasons vary, it has been argued that the use of authentication instead of signatures in services is commonly at the discretion of the service provider and based on risk analysis. In general terms, it can be stated that certain services related to high-risk operations seem to necessitate an electronic signature while the rest may be dealt with on the basis of authentication only.*[37] The associated policy directions affect attitudes to various practical questions surrounding use of e-signatures as well. For instance, if someone has a valid electronic identity but does not possess a device for creating and issuing a valid electronic signature, showing intent online might not even be possible in some cases.

31 The Supreme Court has held, in civil case 3-2-1-151-11, that 'in a contract to which the consumer is the other party, a standard term that provides for the disclosure of a statement of intent contrary to the law and that is detrimental to the other party is unfair' unless either the difference is related solely to the form of expression of the other party's intention or a provision specifies that the address supplied by the other party to the contract to the user of the term may be regarded as the correct address as long as no other address has been communicated to said party. See RKTKo 3-2-1-151-11, 25.4.2012 [12].

32 According to s 7(2) of the LOA, the nature of the obligation and the purpose of the transaction, the customs and practices of the relevant trade or profession, and other circumstances shall be taken into account in the assessment of reasonableness.

33 An e-seal is proof that the e-document has been issued by a legal entity and should provide certainty as to the origin and integrity of the document. While it is not within this article's remit to discuss the legal challenges connected with the time of signing for e-seals, one can conclude readily that similar problems arise. To learn more about the legal framework for e-seals, see L Kask, 'The Electronic Seal As a Solution To Prove the Intent of a Legal Entity' (2021) 30 Juridica International 59. – DOI: https://doi.org/10.12697/ji.2021.30.08.

34 H Hinsberg and others, 'Study on Nordic–Baltic Trust Services' <https://www.digdir.no/internasjonalt-samarbeid/study-nordic-baltic-trust-services/2058> accessed on 1 April 2024.

35 Ibid 48.

36 Those countries being Norway, Sweden, Finland, Iceland, Denmark, Estonia, Latvia, and Lithuania.

37 Hinsberg and others (n 34) 49.

3. Requirements for an e-signature equivalent to signing by hand in EU settings

European Union law too is silent on the time of signature. Prior to the entry into force of the eIDAS Regulation ('the regulation on e-identification and e-transactions'), there was no distinction between levels of e-signatures in Estonia, and such signatures could be divided simply into digital signatures and other electronic signatures. Now, with the eIDAS Regulation, e-signature can be split into several distinct levels of signature provided for therein.[*38] This article focuses primarily on the regulation's provisions dealing with electronic signature that is equivalent to a hand-written signature – i.e., a 'qualified e-signature'.

According to Article 3(12) of the eIDAS Regulation, a qualified e-signature is an advanced electronic signature issued by means of a qualified e-signature-issuing device and anchored in a qualified e-signature certificate. According to the regulation, a qualified e-signature is equivalent to a hand-written signature (per Article 25(2)). Therefore, an electronic signature equivalent to a hand-written signature is an electronic signature that

- complies with the requirements for an advanced e-signature (per Article 26 of the eIDAS Regulation) – i.e., the signature being linked only to the signatory, the signature being capable of identifying the signatory, the signature being issued by means of e-signature data that are only at the disposal of the signatory at a high level of confidentiality, and the signature being linked to the signed data in such a way that any subsequent changes to the data can be identified;
- uses the qualified e-signature-creation tool to create a signature (for example, the chip used for signing must be certified in accordance with Article 30 of the eIDAS Regulation); and
- is based on a qualified e-signature certificate – i.e., it must meet the requirements of Article 28 of the eIDAS Regulation.

Because the regulation is directly applicable, it is impossible to regard an electronic signature that is non-compliant with the requirements for a qualified e-signature that are set forth in the eIDAS Regulation as an electronic signature equivalent to a hand-written signature under national law. The general principle behind the eIDAS Regulation also provides a legal basis for cross-border recognition of e-signatures in the public sector. Where a Member State requires a specific level of e-signature for the use of an Internet-based service provided by or on behalf of a public-sector body, it must likewise recognise e-signatures issued by means of facilities of other countries and service providers, in the format specified in the eIDAS Regulation or using methods specified in the implementing acts for said regulation (see Article 27(2)). Among the implementing acts referred to are the national e-signature implementing acts[*39], which address the standards to which the corresponding e-signatures must be able to be handled by the member states of the European Union. For non-compliant e-signatures, it is up to the country of signature creation to ensure the relevant cross-border processing capability.[*40] What is more, eIDAS 2.0 (see Note 7) will not bring any clarity with regard to the time of signing.

Therefore, European legislation does not create an obligation to determine the time of signature in cases of an electronic signature equivalent to a hand-written signature – i.e., a qualified e-signature. However, it cannot be argued that fixing the time of signature would be in contradiction with the eIDAS Regulation either, since one of the requirements for a qualified electronic signature is that the signature be linked to the signed data in such a way that any subsequent changes to the data can be identified. Also, it can be implicitly inferred from the requirements that some time component of the signature must be fixed, relative to which subsequent changes must be fixed. For Estonia, the national obligation to determine the time of signature is

38 Further information on e-signature levels is available from L Kask, 'E-Eestist e-Euroopasse: elektrooniline allkiri riigisiseses ja piiriüleses suhtluses [From E-Estonia to E-Europe: Digital Signature in National and Cross-Border Communication]' (2017) 10 Juridica 675.

39 Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down the specifications of the advanced e-signature and advanced e-stamp formats pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on e-identification and trust services for electronic transactions in the internal market [2015] OJ L235, 9.9.2015, 37 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006> accessed on 29 March 2024.

40 M Erlich, 'e-Allkirjad Euroopas ja nende käsitlemine Eestis: Juhend ja nõuanded e-allkirjade käsitlemiseks [E-signatures in Europe and Their Treatment in Estonia: A Guide and Advice on Handling E-signatures]' <https://www.ria.ee/sites/default/files/documents/2022-11/EL-e-allkirjade-kasitlemine.pdf> accessed on 29 March 2024.

rooted in Section 80 (3) of the GPCCA. Again, neither the eIDAS Regulation nor national law defines what is to be considered the time of signature, however.

4. Technical components of an e-signature equivalent to a hand-written signature

4.1. Technical creation of an e-signature equivalent to signing by hand

Before one can develop an assessment addressing which of the e-signature operations should be linked to the time of the transaction, one must be familiar with the technical components used to create the e-signature.

The technical creation of a qualified e-signature is guided by numerous international standards, in addition to the requirements of the eIDAS Regulation and the legislation in place that governs transactions. Implementation of international standards ensures that the signature-creation components comply with the requirements laid out in the eIDAS Regulation and provide a high level of security and interoperability of trust services. With respect to the key linked to the e-signature-creation components that is equivalent to that for 'self-signing', the standards of the European Telecommunications Standards Institute (ETSI), as recognised in the implementing act[*41] for the eIDAS Regulation, are central. In Estonia, XAdES e-signatures and ASiC e-signature containers conforming to ETSI standards predominate, but the structure of all the other e-signature formats follows analogous logic.[*42]

If one wants to determine the time of e-signature, it is appropriate to discriminate among the timestamps of three components to the e-signature:

- the fixed time supplied by the e-signature-creation device, such as a personal computer or a service provider's server (denoted as the claimed time);
- the e-signature time that is obtained from the timestamp received from the trust-service provider;
- the time of the request for confirmation of an e-signature certificate's validity (generated via the Online Certificate Status Protocol).

The timestamps associated with these e-signature components are visible to the person in question via the DigiDoc software applied for Estonia.[*43]

The first component mentioned above, the fixed time from the device or the server of the service provider used by the person to e-sign, employs a value set at the time of e-signing (PIN2 or PIN entry for e-signing). Technically, this is the time the device has captured for when the signatory 'claims' to have e-signed.[*44] The time fixed by the e-signature-creation tool or the service provider's server is stored in the e-signature container when the PIN2 value or signature PIN is entered, and the signature created thereby cannot be changed without harm to the technical signature chain. At this juncture, it is necessary to immediately consider the fact that the fixed time from the e-signature-creation device might not be accurate. A person can change the time on his or her device manually, in addition to which the accuracy of the timestamp generated by that device can be affected by external factors without the user's knowledge. The fixed time from the e-signature device could be compared especially pertinently to the date someone marks in the

41 According to Commission Implementing Decision 2015/1506 (n 33), the advanced e-signatures referred to in art 1 must comply with one of the ETSI technical specification sets mentioned in the decision.

42 'Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures; Part 1: Building Blocks and XAdES Baseline Signatures' (ETSI EN 319 132-1 v. 1.1.1, April 2016) <https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf> accessed on 29 March 2024; 'Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building Blocks and ASiC Baseline Containers' (ETSI EN 319 162-1 v. 1.1.1, April 2016) <https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf> accessed on 29 March 2024. In addition to DigiDoc, components are visible through alternative e-signature validation applications.

43 DigiDoc software allows the user to open digitally signed documents, check the validity of signatures, and digitally sign and encrypt data. See the software's documentation from the State Information System Authority, 'eID lõppkasutaja rakendused' <https://www.ria.ee/et/riigi-infosusteem/eid/digidoc-tarkvara.html> accessed on 28 February 2024.

44 The ETSI standard describes the time fixed by the e-signature facility thus: 'The SigningTime qualifying property's value shall specify the time at which the signer claims to hav[e] performed the signing process.' See 'Electronic Signatures and Infrastructures … XadES' (n 42) para 25.

signature block of a physical document to be signed: the date marked may or may not coincide with the actual time of signature.

The second time component, from the timestamp[*45] request to the trust-service provider, gets created immediately after the signer enters PIN2, which is required for the signature to be created.[*46] The timestamp serves to associate the electronic signature data with a specific point in time, so as to prove the existence of the transaction and the e-signature data at the time of the timestamp request. A timestamp can be likened to an envelope in the analogue world, with information inside and a stamp on the outside postmarked to indicate roughly when the information was put inside. It cannot be used as proof of when the information itself was documented. Although Estonian practice equates the time of the timestamp request with the time of the signature, one must recognise that the timestamp request cannot be used to verify what world time[*47] was in force at the moment when the person confirmed their will by entering their PIN2. The timestamp query indicates a fixed time reflecting the actual time of the world, but the event preceding it – the basic signing – has already taken place.[*48]

Thirdly, since a qualified e-signature is valid only if the qualified e-signature certificate is valid at the time of issuance, a validity-confirmation request is placed with the trust-service provider after the timestamp request, to check the validity of that certificate. The validity-confirmation query allows requesting information on the validity of certificates in real time – but only this. Hence, the query does not retrospectively address whether the certificate was valid at either the time stated by the e-signature facility or the time of the timestamp request; it covers purely the validity of the certificate at the time of the request.[*49] For an additional technical verification measure, the DigiDoc software compares the timestamp from the e-signature facility with the timestamp connected with the validity confirmation query. If there is a mismatch (a difference of more than 15 minutes), the signature-generation chain is broken, and a qualified e-signature container cannot be created.

In Estonia, all three components are used, in the order presented above, for the creation of an e-signature, and the timestamps from all three components are stored in the associated, set sequence in the e-signature container. In the 'front-page' view of the e-signature container, the Estonian DigiDoc software displays the time of the timestamp request as the time of e-signature creation, while a detail-level view of the container shows all three times. Since the timestamp request and the validation request are, in accordance with Estonian best practice, made immediately after PIN2 is entered via the e-signature device and the time between the timestamp request and the certificate-validation request hence cannot reasonably be more than 15 minutes, all three components generally refer to the same date, so disputes about the date of signature very seldom arise.

However, in the case of an e-signature that has already been created, it is possible to perform a timestamp enquiry and a validity-confirmation query again. After that later point, the timestamps stored in the e-signature container get updated[*50], while, the initial time from the e-signature device is preserved, unaltered. At present, though, the author is not aware of anyone, outside theoretical studies, who has distorted the true facts of the transaction by re-timestamping the e-signature or by querying the validity of the e-signature such that legal disputes have ensued. Furthermore, doing so has no practical value anyway,

45 The eIDAS Regulation's art 3(33) states that 'electronic timestamp' means data in electronic form that bind other data in electronic form to a particular time, thereby establishing evidence that the latter data existed at that time. The technical solutions permit a situation wherein the signature may have been provided at any time before the time indicated in the timestamp, provided that the signature-creation data and the corresponding certificate already existed at that time. For a solid understanding of the various technological challenges connected with this, the reader is directed to the doctoral dissertation of A Parsovs, 'Estonian Electronic Identity Card and Its Security Challenges' <https://cybersec.ee/storage/phd_idcard.pdf> accessed on 28 February 2024.

46 In the previous system, using TimeMark signatures, the timestamp request was merged with the validity-confirmation request.

47 For more information on world times, in Estonian, see 'Maailmaaeg' <https://et.wikipedia.org/wiki/Maailmaaeg> accessed on 28 February 2024.

48 The ETSI standard defines timestamp requests in the same way: the term '"electronic time stamp" means data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time […]. Containers for electronic time-stamps proving that some or all the signed data objects have been created before [a] certain time instant.' See 'Electronic Signatures and Infrastructures … XAdES' (n 42) para 5.3.

49 The nature of the certificate-suspension scheme renders it impossible to obtain information on whether a certificate was valid at a specific instant any time in the past through a validity-confirmation query.

50 Mets and Paršovs (n 9) 44.

since the e-signature container in the possession of the person making the declaration of intent in the case of a multilateral transaction can be used by the latter person to prove when the request was actually made, and, furthermore, making a declaration of intent in an electronic environment always necessitates utilising some medium or channel to deliver the declaration of intent, which applies its own stamping/logging. Even if the person making the declaration does not have the original container of the e-signature any longer, it is possible to request the necessary information from the trust-service provider, who is responsible for maintaining a record of the timestamp requests and validation requests. This is not discretionary: under Section 5 (3) of the Electronic Identification and Trust Services for Electronic Transactions Act*[51] (EUTS), a qualified trust-service provider is obliged to document the activities carried out during its provision of the trust service and to keep a record of these activities for a period of 10 years from the creation of the record. In this connection, it is important to stress that a later request cannot change the time of the timestamp request in the e-signature container from the original one when adding the time of the new request. This is a vital aspect of the infrastructure.

4.2. Establishing the link between an e-signature equivalent to hand-signing and the time of the transaction

The requirement for a link to the time of e-signing is derived from Section 80 (3) of the GPCCA, discussed above. In the case of the three time components described in Subsection 4.1, distinctions must be drawn with regard to the manner of linking to the time of the transaction. At the moment at which the person e-signing enters the PIN2 value and the timestamp generated by the e-signature-creation device is fixed, an invariable, complete chain is created that links the identity of the signatory, the time stored by the e-signature-creation device, and the content of the transaction. In legal terms, an e-signature thus created fulfils the conditions for an electronic-form transaction that are set out in Section 80 (2)–(3) of the GPCCA (with the reservation that the time recorded by the e-signature device may not be accurate). Since the time of the e-signature cannot be considered wholly reliable, the practice in Estonia is to take the time of the timestamp request instead as the time of the qualified e-signature. The time of that request corresponds to the actual Universal Time (i.e., Greenwich Mean Time) point at which the transaction and the e-signature data were verified.

Alternatively, one could consider the time of requesting validity confirmation for the qualified certificate for the e-signature to be the time of e-signature issuance, because at that moment there exists, in addition to the timestamp, confirmation of the validity of the certificate. While the certificate-validity-confirmation query plays a central role in the validity of the qualified e-signature – in that this query is important for proof that the certificate is valid and that the e-signature issued meets the conditions for a qualified e-signature – it should not, however, be considered the time of issuance of the e-signature.

It follows from the foregoing reasoning that linking the act of e-signature to the time of the transaction within the meaning of the GPCCA's Section 80 (3) is problematic and requires consensus. The search for a solution is made more difficult by the fact that the legislator's intention in linking the e-signature to the time of the transaction is unclear in substance. Questions arise as to which fixed point in time from a component should constitute the link to the time of the transaction, and in what way, with the distinct levels of e-signatures being taken into account also.

Linking the time of the e-signature to the time of the transaction has long formed the starting point in Estonian practice for e-signatures equivalent to hand-written signatures. Therefore, from the standpoint of legal certainty (but also from the perspective of the reliability of transaction execution), the author does not consider it expedient to abandon fixing of a time associated with the e-signature altogether. One possibility could be to consider interpreting the mandatory time component articulated in the current Section 80 (3) of the GPCCA as a timestamp request whereby the person can prove, in addition to the existence of the transaction and the e-signature data, the declaration of intent having truly been made. At the same time, it should be borne in mind that lower-tier e-signature mechanisms are in circulation, ones for which there is no requirement to bind the time of making the declaration of intent to the time of the transaction. Alternatively, the time set by the e-signature-creation device could be considered sufficient (since lower-tier e-signatures do not entail making any additional requests to trust-service providers). A final consideration is that it is

[51] E-identimise ja e-tehingute usaldusteenuste seadus: RT I, 25.10.2016, 1; RT I, 12.12.2018, 30.

impractical to waive the requirement for some time of signature: having a precise time of signature allows signatures to be machine-processed in an integrated, automated fashion. For automatic data exchange, information systems must be able to rely on agreed time formats.

Given that the eIDAS Regulation does not, as Section 80 (3) of the GPCCA does, require linking of the e-signature to the time of the transaction, the appropriateness of the Estonian legislator requiring this in such an imperative form is cast into doubt, though. If, when the eIDAS Regulation entered into force in 2016, the system of e-signatures regulated by the Digital Signatures Act had been reorganised, the legislator could also have considered revising the regulation of electronic-form transactions directly related to the e-signature. In addition, one should remember that, while the legal obligation for cross-border recognition of e-signatures equivalent to hand-written signatures stems from the eIDAS Regulation, the process of creating an e-signature is structured differently from country to country. Both the content of the e-signature container and the technical process of creating an e-signature may differ greatly.[*52]

5. Practical problems in identifying the time of e-signing equivalent to hand-signing

5.1. The time-verification impact of suspending the certificate for e-signature equivalent to hand-written signature

If someone has lost their e-signature document, it has been stolen, or the person suspects that it may be misused, the certificates connected with the source electronic document can be suspended. The certificate is electronic proof that links the data necessary to authenticate the person and the digital signature and that confirms that person's identity. In the case of mobile identification solutions, the certificates are not stored on the SIM card. As with ID-card-based solutions, these utilise two certificates, one for authentication and the other for signing.[*53]

Articles 28(5) and 38(5) of the eIDAS Regulation give Member States the right to introduce national rules that take into account the regulation's requirements, with eIDAS Recital 53 going on to explain that suspension of qualified certificates is a well-established practice among trust-service providers in several Member States. This differs from revocation in that it only leads to the temporary invalidity of the certificate in question. The provisions that the EUTS makes for suspending a certificate are similar to those previously found in Section 12 of Estonia's Digital Signature Act[*54]. According to Section 9[5] of the former IDA, the issuer of the document (the Police and Border Guard Board and the Ministry of Foreign Affairs) may, under the conditions set out in sections 17 and 18 of the EUTS, suspend the certificate tied to the identity document and restore the validity of a suspended certificate. With the former, the EUTS gives the trust-service provider the right to suspend the validity of a trust-service certificate if there is a suspicion that false data have been entered for the certificate or that the private key corresponding to the public key held in that certificate can be used without the consent of the certificate-holder (see Section 17 (1)). Correspondingly, according to the explanatory memorandum on the EUTS, discretion to suspend a certificate is granted to the trust-service provider if there is a suspicion that incorrect data have been entered for the certificate or that a private key corresponding to the public key contained in the certificate can be used without the consent of the certificate-holder. A formal procedure involving filing a petition is not appropriate in these cases, because certificates may have to be suspended swiftly if major damage is to be prevented (e.g., if an ID card and the associated PINs are lost), and expeditious means must be possible – for example, involving a telephone call. Processing an application, in contrast, is a longer and more time-consuming procedure.[*55]

52 For reasons of space, the technical components of e-signatures in individual countries and their national legislation on signature timing are not examined in this article.

53 State Information System Authority, 'Sertifikaadid [What Certificates Are]' <https://www.id.ee/index.php?id=30228> accessed on 29 March 2024.

54 Digitaalallkirja seadus: RT I 2000, 26, 150; RT I, 14.3.2014, 12 (invalid).

55 See the explanatory memorandum on the draft act for the law on e-identification and e-transaction trust services, 237 SE: 'E-identimise ja e-tehingute usaldusteenuste seadus 237 SE' <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/323afaca-cb96-4118-a675-2a2db388141e/> accessed on 29 March 2024.

In the interests of legal certainty, it is necessary that the status of the certificate (valid, suspended, or invalid) always be clear, which is why a validity-confirmation check is carried out for the certificate, the time of which is captured for the e-signature container. In the case of suspension of a certificate, trust-service providers has to honour an obligation to indicate the exact span for which the certificate has been suspended.[*56] Pursuant to Section 17 (3) of the EUTS, once a certificate has been suspended, the trust-service provider must promptly enter the details of the suspension in the certificate database it maintains and must keep records of the timing, reason, and applicant connected with the suspension and any termination of that suspension. Consequently, whenever a trust-service provider suspends certificates, a specific span of time during which the certificates remain suspended shall be specified, case-specifically.[*57] Technically, it is possible to begin creation of an e-signature even if the certificate is suspended, since the e-signature-creation tool can create a basic signature and can perform a timestamp request, but the maximum time lag that Estonia specifies between a timestamp request and a request for confirmation of the validity of a certificate renders it highly unlikely in practice that the certificate was in a suspended state at the time of the timestamp request but its validity had been restored by the time of the confirmation request. There is no expectation of ultimately generating a qualified e-signature when one starts with a suspended certificate.

For querying the suspension status and validity of a certificate, a check involving validity confirmation for the person's certificate is made against the certificate database maintained by the trust-service provider (e.g., SK ID Solutions AS in Estonia); this prompts a procedure checking whether the certificate used to issue the e-signature was valid at a specific point in time, and the time of this status query gets added to the e-signature container. Because the conditions for a qualified e-signature require that the e-signature certificate be valid at the time of that e-signature (i.e., at the time of e-signing equivalent to signing by hand), issuing an e-signature with a suspended certificate is rendered impossible, and any e-signature somehow issued while a certificate is suspended is invalid according to Section 17 (5) of the EUTS. Suspension of a certificate generally occurs only in isolated cases, but Estonia has experienced large-scale certificate suspensions too: in 2017's 'ID-card crisis'[*58] caused by the ROCA vulnerability, 760,000 individuals had their ID-card certificates suspended.[*59] Although it could be argued that the permissibility of suspension is one of the main factors enabling remote renewal of one's ID card, without individuals having to exchange documents physically, recent discussions have nonetheless led to a proposal to cancel the option of suspension.

The draft law to amend the IDA[*60] includes elimination of the possibility of suspending these certificates. The main reason is the existence of a theoretical possibility of creating a cryptographic signature with a suspended certificate such that, when the validity of the certificate is restored, it is not possible to identify that the signature was produced while the certificate's validity was under suspension.[*61] This scenario runs counter to the requirement stated in Article 32 of the eIDAS Regulation with regard to the validation of a qualified e-signature, because there is no way to verify with full certainty whether the certificate was indeed valid at the time of signing. Should the newly proposed amendments be adopted, the possibility of suspending and later restoring the validity of a certificate therefore will no longer exist for any identity documents issued under the IDA, from 1 November 2025 onward.

Since suspension has been employed as a convenience measure in the lightweight process described above, researchers have sought to prove that the same level of convenience can be reached by means of the revocation mechanism. They have answered in the affirmative, assuming the use of a technical solution that allows the signer to obtain a new certificate without having to replace the existing qualified-signature-creation device.[*62] So far, solutions of this kind have been utilised only to rectify security flaws.

56 See the eIDAS Regulation's recital 53.

57 K Laanest and L Kask, 'ID-kaardi turvarisk: Õiguslikud probleemid [Legal Issues Related to ID-Card Security Risk]' (Tallinn, 2017) <https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/id-kaardi-turvarisk-oiguslikud-probleemid.pdf> accessed on 28 February 2024.

58 For more information on suspension of certificates and on termination of that suspension, see Laanest and Kask (ibid).

59 For details, see the ID.ee page on Estonia's suspension of nearly 760,000 ID-card certificates from the evening of 3 November 2017 (2 November 2017) <https://www.id.ee/index.php?id=38339> accessed on 28 February 2024.

60 A list of IDA amendments is available online, under the heading 'Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadus' (23 January 2024) <https://eelnoud.valitsus.ee/main#fHAkf6ru> accessed on 29 March 2024.

61 Ibid. See the explanatory memorandum's para 18.

62 Mets and Paršovs (n 9) 49.

5.2. Agreement on identifying the time for an e-signature equivalent to a hand-written signature

In practice, problems may arise in situations wherein the entry into force of a contract or the time at which it is deemed to have been concluded is linked to the time at which e-signing is performed. According to Section 11 (2) of the LOA, a contract shall not be deemed to have been concluded before it has been given any prescribed form specified by agreement between/among the parties or requested by one of the parties as the form in which the contract must be concluded. According to Article 25 of the eIDAS Regulation, an e-signature shall not be declared legally invalid or inadmissible in legal proceedings merely because it is in electronic form or does not meet the requirements for an e-signature equivalent to a hand-written signature – i.e., for a qualified e-signature. Associated common practice is not to express the time in the letter of intent or the contract but to use wording such as 'the contract is deemed to have been concluded upon digital signature' or 'the contract takes effect upon digital signature by both parties' and leave it to the parties to determine the time of signature. This approach is supported by Section 11 (4) of the LOA, under which a written contract is deemed to have been concluded when the contracting parties have signed the contract document or have exchanged contract documents or letters signed by both parties. If the time of signature is undefined and technically expressed with significantly different timestamps, a question may arise as to whether the contract has entered into force or at least when the contract must be fulfilled. Whilst the date is generally sufficiently relevant for determining the time, there may exist time-critical agreements whose time of signature makes it possible to ascertain whether a party to the transaction was late with finer granularity. Any inter-party practice established, alongside the channel through which the statement of intent or contract is presented to another party, plays an important role here. One possibility, however, is to indicate in the letter of intent or the contract the time from which the parties wish the legal consequences to be realised.*[63] Since the timestamp request and the validation request get made immediately after the PIN2 credential is entered to the e-signature device and the timestamp request and the request for validation of the certificate cannot be more than 15 minutes apart, the times of all three components generally coincide such that there is usually no dispute about the date of signature. Where minutes too are relevant for a fact subject to dispute, the author considers it the most reasonable to rely on the time of the timestamp request, which points to the actual time in the world, to pinpoint the time at which the person expressed their will and whether it was related to the circumstances underlying the expression of that will.

6. Conclusions and implications

The central conclusion from comparing signing and timing in the analogue world with their equivalents in an electronic environment is that, as a rule, determination of the time of signature is not necessary from the perspective of the legal consequences and is not required by law. From a civil-law point of view, when the agreement-expressing document was drawn up is irrelevant and the formalisation of an agreement subsequently as a document does not preclude the timing-related legal consequences. While signing by hand is necessary for compliance when a written-form requirement exists and while said signature should be placed at the end of the transaction document to indicate the content and scope of the transaction, a hand-written signature is not legally defined and stating the time of signature is required only in those cases for which the law renders it mandatory. In an electronic environment, contrastingly, the requirement to sign does necessitate specifying the time of signature. Nevertheless, no definition is given for the time of signing and, as in the analogue world, it is necessary to assess the behaviour of the person in question, in conjunction with the custom and practice previously established or agreed upon between/among the parties, to evaluate the real intention of the person.

Neither the eIDAS Regulation nor the recent amendment of the EU's regulation on European electronic signatures mandates setting a time for signing. In addition, the GPCCA requiring a time for signature does not contradict the eIDAS Regulation, since the latter regulation can be read as entailing an implicit requirement for a fixed time component. As for which of the e-signature operations should be linked to the

[63] T Mets and A Paršovs (n 9) have also come to the conclusion that the legally relevant dates (time) could still be indicated in the document to be signed.

time of the transaction, the paper's analysis focusing on the process of creating an e-signature equivalent to a hand-written signature provides a starting point.

The linking of the act of e-signature to the time of the transaction within the meaning of Section 80 (3) of the GPCCA is not defined in substance. From the legal-certainty standpoint and in the interest of smooth and reliable execution of transactions, it is not expedient to waive fixing of a time for the e-signature. Still, consideration should be given either to amending the law or to interpreting the practice in such a way that the time of the timestamp request could be regarded as the mandatory time provided for by Section 80 (3) of the GPCCA. Although technical shortcomings would still remain, accepting the proposed elimination of the possibility of suspending the certificate for electronic signature would help to overcome the technical possibility of discrepancies related to time spans for which signature are not valid. Also, since the eIDAS Regulation mandates a certain level of cross-border recognition of e-signatures, cross-border practice should certainly be taken into consideration. As analysis of conditions in the Nordic–Baltic region revealed, the signer might not even have an electronic-signature-creation device, and many of the region's operators and countries deem authentication together with the technical logs for transactions sufficient to attest to intent in an electronic environment. Conditions such as these certainly are affecting the evolving practice of using e-signatures in both national and cross-border transactions.