ARTICLE:

Time of signing in the Estonian digital signature scheme

By **Tõnu Mets and Arnis Parsovs**

There is a widespread misconception among some lawyers, technologists and the public that the Estonian digital signature scheme[1] provides reliable proof of the time when a document was digitally signed. In this article we show that the legal requirement to establish the time of signing is not met in practice. The related legal requirement that the validation of the digital signature should confirm that the certificate was valid at the time of signing is also not met. We analyse the legal consequences of this, and discuss possible solutions for the issues that arise. We note that digital signature schemes used in other countries implementing Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014[2] (eIDAS) are likely to share the problems discussed in this article.

Background

The Estonian digital signature scheme is considered to be one of the most successful implementations of an electronic signature scheme in Europe. The national Digitaalallkirja seadus (Digital Signatures Act)[3] (DSA) implementing eSignature Directive 1999/93/EC[4] (Directive) came into force on 15 December 2000, and the first digital signature was issued in 2002. The law gave the digital signature the equivalent legal effect of a handwritten signature. The Estonian DSA regulated electronic signatures that, in the context of the Directive, were recognized as advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device. The current eIDAS recognises them as qualified electronic signatures. The DSA was replaced by the E-identimise ja e-tehingute usaldusteenuste seadus (Electronic Identification and Trust Services for Electronic Transactions Act)[5] (EITSETA), which is a national implementation of the eIDAS regulation.

The significant factor that enabled the widespread use of digital signatures was the inclusion of the signature creation data inside an electronic identity card (ID card) that is issued by the state as a mandatory identity document for all Estonian residents aged 15 and above.[6] Recently, in the context of the e-residency programme,[7] non-residents are also provided with a qualified signature creation device (QSCD), which can be used to provide a qualified electronic signature.

When introducing the digital signature scheme, Estonia introduced the XML-based digital signature file format DDOC (DigiDoc). Recently, the DDOC format has been updated to the BDOC[8] format that complies with the eIDAS digital signature format based on XAdES and ASiC standards. The BDOC format (.bdoc or .asice file extension) is the standard used today for digital signatures in Estonia, while other digital signature formats are not used in practice. The Estonian Information System Authority provides software libraries and standalone applications for the creation and validation of signatures.

[1] The term 'digital signature scheme' used in this article refers to the organisation and system of using electronic signatures with the legal effect of handwritten signatures in accordance with article 25(2) of eIDAS. It also includes the related concept of the digital seal ('qualified electronic seal' in the context of eIDAS).

[2] Regulation (EU) No 910/2014 of the European Parliament and 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, 28.8.2014, p. 73-114.

[3] RT I 2000, 26, 150. Repealed on 26.10.2016. English translation of the last wording in force before being repealed: https://www.riigiteataja.ee/en/eli/ee/508072014007.

[4] 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, 19.1.2000, p. 12-20.

[5] RT I, 12.12.2018, 30, in force from 26 October 2016. English translation: https://www.riigiteataja.ee/en/eli/511012019010.

[6] The person is bound to the digital signature through a qualified certificate, which contains data such as the name and the unique personal identification code of the person. When issuing the certificate, the identity of the person is verified by physical presence, in accordance with the provisions of eIDAS article 24(1).

[7] For more on the Estonian e-Residency programme, see https://e-resident.gov.ee.

[8] BDOC – Format for Digital Signatures. Version 2.1.2:2014. http://www.id.ee/public/bdoc-spec212-eng.pdf.

With the introduction of the national legal framework for digital signatures, the Estonian lawmaker added the requirement that the digital signature must establish the time when the signature was given. Consequently, the graphical interface of the signature validation application has a 'Signed on' field next to the signatory's name to display the time when the signature was purportedly given. However, as highlighted in this article, the time shown in the signature validation application does not reflect the actual time of signing. This results in a digital signature scheme that does not comply with the legal requirements. The focus of this article is the analysis of this failure to comply and the resulting problems.

Time of signing in law

The requirement of time of signing for electronic signatures[9] is established in the Tsiviilseadustiku üldosa seadus (General Part of the Civil Code Act)[10] (GPoCCA) subsection 80 (3):

> 'Elektrooniline allkiri peab olema antud viisil, mis võimaldab allkirja seostada tehingu sisu, tehingu teinud isiku ja tehingu tegemise ajaga.'
>
> 'An electronic 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.'

According to the explanatory memorandum of the draft legislation of GPoCCA, this was supposed to define the general prerequisites when an electronic signature could be considered equivalent to a handwritten signature, with further details specified in a more thorough regulation on digital signatures.[11] Interestingly, the first draft of GPoCCA did not require the signature to be associated with the time of entry into the transaction.[12]

The requirement of the time of signing was introduced in the legal definition of the digital signature in clause 2(3)(2) of the DSA, which required the digital signature scheme to enable the determination of the time when the signature is given. According to the explanatory memorandum of the DSA, every digital signature is given a timestamp using cryptographic methods, which proves the time of signing.[13]

Therefore, the time of signing in Estonian law is considered to be an essential characteristic of a valid digital signature. The requirement to establish the time of signing is meant to add a higher evidentiary value to a digital signature than manuscript signatures on paper documents can provide. In addition, and more importantly, the requirement aimed to establish whether the signature was given during the validity period of the signatory's certificate and hence to determine whether the given signature is legal and valid. The law does not provide a definition of time of signing. However, for the time of signing to serve its legal purpose, it must correspond to the moment when signature creation data is used.[14] We note, however, that the validity of a certificate at the time of signing can be established without establishing the precise time of signing. For example, if it can be established that a signature was given before the certificate associated with it has expired or was revoked, it can be concluded that at the time of signing the certificate was valid (exceptions are analysed later in the article).

Additionally, a presumption of authenticity for all digitally signed documents is included in subsection 277(3) of the Tsiviilkohtumenetluse seadustik (Code of Civil Procedure) (CoCP).[15] This presumption of authenticity is based on the trustworthiness of the

[9] A digital signature is a type of electronic signature regulated by law. Other possibilities that can be construed as forms of electronic signature include fingerprints, retinal scans, iris patterns, face recognition and voice prints, which are not recognised in practice in Estonia.
[10] RT I, 30.01.2018, 6. English translation: https://www.riigiteataja.ee/en/eli/502012019003.
[11] Tsiviilseadustiku üldosa seaduse eelnõu seletuskiri (Explanatory Memorandum for Draft Legislation of General Part of the Civil Code Act). Tsiviilseadustiku üldosa seadus (121 SE I) Tallinn, 1999: https://www.riigikogu.ee/download/621749a1-55dc-3f8e-a492-b3c586856a00.
[12] Archive of Ministry of Justice, Fond 1, nim 2, s 4024, l 23.
[13] Seletuskiri digitaalallkirja seaduseelnõu juurde (Explanatory Memorandum for Digital Signatures Act). Digitaalallkirja seadus (151 SE) Tallinn, 1999: https://www.riigikogu.ee/download/f2f6398a-30ab-337e-b6d4-40d30b64186a.
[14] For the Estonian ID card, this corresponds to the moment the signatory authorises signature creation by entering their PIN.
[15] RT I, 19.03.2019, 22. English translation: https://www.riigiteataja.ee/en/eli/512042019002.

Estonian digital signature scheme.[16] Therefore, when an electronic document bearing a digital signature is presented as evidence in civil proceedings, its authenticity is presumed.

The Regulation (eIDAS) entered into force on 1 July 2016. The Regulation is directly applicable to member states. eIDAS article 25(2) gives qualified electronic signatures the equivalent legal effect of handwritten signatures. Contrary to Estonian law, the definition of the qualified electronic signature in eIDAS does not require the time to be established when a digital signature was given.

In the Estonian Supreme Court judgement of 3-15-1188 of 27 September 2017,[17] the Administrative Chamber of the Supreme Court found that given the primacy of European Union law over Estonian national law, the latter cannot affect the applicability of the former. Due to the direct applicability of eIDAS, the requirement in Estonian law to establish the time when a digital signature is given no longer applies from 1 July 2016. This important legal change, however, has not received public attention. The common belief remains that eIDAS did not change the legal status of Estonian digital signatures.

On 26 October 2016, the DSA was replaced with EITSETA. The EITSETA does not provide the definition of a digital signature, but refers to the definition of the qualified electronic signature as set out in eIDAS. According to clause 25(1)(3) of EITSETA, digital signatures given before EITSETA entered into force are considered valid when certain prerequisites are met, one requirement being that it is possible to determine the time when the signature was given. Therefore determining the time of signing is vital for every digital signature given via the Estonian digital signature scheme before 26 October 2016 for the signature to have the equivalent legal effect of a qualified electronic signature. We note, however, that this requirement to determine the time of signing conflicts with eIDAS, and cannot apply to digital signatures given after 1 July 2016.

The definition in GPoCCA subsection 80(3) concerning digital signatures was not updated after eIDAS came into force. It still requires the time of entry into the transaction to be determined. This requirement, however, conflicts with eIDAS and cannot apply to digital signatures given after 1 July 2016.

Time of signing in the digital signature scheme

Contrary to the law and common belief, the Estonian digital signature scheme has never provided reliable proof of the time when a signature was given. The 'Signed on' time shown by the signature validation application is taken from the electronic timestamp issued by a qualified trust service provider.[18] However, contrary to the DSA explanatory memorandum, the time embedded in the electronic timestamp does not provide proof of the time when the document was signed. The timestamp, as set out in article 3(33) of eIDAS, provides only the proof that the data (the digital signature) already existed at the time specified in the timestamp. In reality, the signature may have been given at any time before the time shown in the timestamp, providing the signature creation data and the corresponding certificate already existed at that time.

Since a valid[19] timestamp can be obtained by parties other than the signatory at any time after the signature has been given (as long as the signatory's certificate at the time of obtaining timestamp is valid), the signing time shown by the validation application cannot be trusted to establish the time when the signature was given. Therefore, the 'Signed on' time that is currently displayed by the graphical interface of the signature validation application should be interpreted to mean 'Signed before' or 'Validity confirmed on' time.

According to the technical standards, a signatory's self-reported[20] computer time has to be included in the signed metadata, and can be found by inspecting the technical details of the signature. However, since

[16] A. Kangur. § 277, 3.8.2. – Tsiviilkohtumenetluse seadustik I. Kommenteeritud väljaannne (Commentaries of the Code of Civil Procedure). Tallinn: Juura 2017.
[17] RKHKm 27.09.2017, 3-15-1188.

[18] Digital signature formats used in Estonia implement LT-Level conformance (Signature with Long-Term Validation Material) of AdES ETSI standard, where the signature container contains the timestamp of the signature and OCSP response.
[19] Technically meaning a timestamp of a signature that is accompanied with OCSP response proving that after the timestamping the signatory's certificate was still valid.
[20] 'SigningTime' element. BDOC – Format for Digital Signatures. Version 2.1.2:2014. http://www.id.ee/public/bdoc-spec212-eng.pdf, p 9 and ETSI TS 101 903 V1.4.2 (2010-12). Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES). Technical Specification.http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf, section 7.2.1.

at the time of signing the signatory can set this time to an arbitrary value, it cannot be used to establish the time of signing either. While the problem of establishing the time of signing in a trusted manner is well known by the designers of the digital signature scheme and is clearly documented in the Estonian digital signature file format specification,[21] the legal system and the processes built around the Estonian digital signature scheme ignore this shortcoming.

Establishing certificate validity at the time of signing

While establishing the time of signing is not required by eIDAS, article 32(1) of eIDAS requires the validation process of a digital signature to confirm the state of several properties at the time of signing. Namely:

> (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with annex I of eIDAS;
>
> (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
>
> (h) the requirements provided for in article 26 of eIDAS were met at the time of signing.

The question arises whether a digital signature scheme that does not provide reliable proof of the time of signing can provide reliable proof of the fulfilment of these requirements at the time of signing.

While the timestamp attached to a digital signature does not prove that the signature was given at the time specified in the timestamp, the timestamp does prove that the signature was given before the time specified in the timestamp. Hence, if the state of the properties required for validation can change only from a valid state to an invalid state, but not vice versa, then the timestamping mechanism would allow the establishment of proof of validity at the time of signing.

For example, we can imply that the validation requirement of article 32(1)(h) of eIDAS, among other things, requires assurance that the cryptographic algorithms used to create the signature were considered secure at the time of signing. When an algorithm is found to be insecure, the algorithm cannot be later found secure again. Therefore, where a timestamp proves a signature existed at the time when the algorithm was considered secure, it will also prove the property that, at the time of signing, the signature algorithm was not broken.

The same applies to validation requirement of article 32(1)(a) of eIDAS. A qualified certificate is qualified from the beginning of its issuance, and once it loses its qualified status (for example because the qualified trust service provider is deleted from the registry of qualified trust service providers), the same certificate cannot become qualified again. The problem lies within the validation requirement of article 32(1)(b) of eIDAS, which requires assurance that the certificate was valid at the time of signing. EITSETA and eIDAS define two cases where a certificate can change its status from an invalid certificate to a valid one.

The first case is described in EITSETA subsection 16(4):

> 'Sertifikaat hakkab kehtima selles märgitud kehtivusaja algusest, kuid mitte enne sertifikaadi andmete kandmist selle väljaandja peetavasse sertifikaatide andmebaasi.'
>
> 'A certificate is valid from the beginning of the period of validity set out in the certificate but not before the data of the certificate are entered in a certificate database kept by the issuer of the certificate.'

In practice, after being technically issued, the certificate is registered as invalid in the database of the trust service provider. However, the validity status is changed to valid after the signature creation data is delivered to the signatory. In the context of EITSETA, this is not certificate validity suspension,[22] but a separate 'not yet valid' status. The suspension of a certificate is regulated separately. The provision that the certificate after its creation could be considered invalid until its activation is also foreseen in article 28(4) of eIDAS: 'If a qualified certificate for electronic signatures has been revoked after initial activation [---]'.

[21] BDOC – Format for Digital Signatures. Version 2.1.2:2014. See: http://www.id.ee/public/bdoc-spec212-eng.pdf, section 6, paragraph 3.

[22] For example, the Lithuanian law, Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų (Law on Electronic Identification and Trust Services for Electronic Transactions), requires the trust service provider to suspend the certificate until the signature creation data is delivered to the signatory, for which see article 12(1)(5).

The second case is described in EITSETA sections 17 and 18. EITSETA permits the validity of a certificate to be temporary suspended, later terminating the suspension and making the certificate valid again. Additionally, EITSETA subsection 17(5) explicitly states:

> 'Sertifikaadi kehtivuse peatatuse ajal antud e-allkiri või e-tempel on kehtetu.'
>
> 'E-signatures or e-seals given during the period when a certificate is suspended are invalid.'

The EITSETA provisions are based on similar provisions in eIDAS article 28(5).

As we noted above, we gave examples of two cases where a certificate can change its status from non-valid to becoming valid. This means the timestamp of the signature obtained when a certificate is valid will not conclusively prove that the signature was given at the time when the certificate was valid. In practice, the signature could have been given while the certificate was not valid, but a valid timestamp could have been obtained later after the certificate became valid.

To conclude, because of these two cases, the validation process of the Estonian digital signature cannot provide assurance that a digital signature was given at the time when the certificate was valid. It follows that the validity of a digital signature produced by the Estonian digital signature scheme cannot be verified.

The same problem applies to the digital signatures of any EU member state where certificate validity suspension is implemented, or where certificates do not become valid from the moment of their issuance. This is because the eIDAS technical standards[23] currently do not provide a mechanism that would satisfy the eIDAS legal requirements for signature validation in these cases. While eIDAS does not require member states to support certificate validity suspension, we found only Slovakia[24] prohibiting the suspension of certificate validity.

Implications

Transactions relying on the time of signing

The parties entering into a contract using digital signatures are usually not aware that the digital signature scheme does not provide a reliable means of establishing the time of signing. Therefore, a common practice for agreements signed digitally is to not have an explicit date specified in the signed document itself, but instead to refer to the time of the digital signature. For example, it is becoming common practice to state in the signed document that it enters into force from the time of signing.

While the original digital signature container can be used to prove the earliest time of the existence of the signature, a malicious party can create a modified signature container with an updated timestamp and deceive a third party who does not have access to the original signature container with the earliest timestamp.[25] Therefore, the practice of referring to the time the document is digitally signed in order to determine the date of a digitally signed document should be abandoned. All legally significant dates should be specified in the electronic document to be signed.

Contesting the validity of digital signature

Where a digital signature scheme does not satisfy the legal requirement of establishing the time of signing and fails to establish certificate validity at the time of signing, the validity of a digital signature attached to electronic document can be contested.

Currently there is no technical standard describing the algorithm for validating a qualified electronic signature in respect to the legal requirements set out in eIDAS Article 32(1).[26] Similarly, the BDOC format specification does not provide a precise algorithm for

[23] 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 eIDAS, OJ L 235, 9.9.2015, p. 37–41.

[24] Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) (Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendment and Supplementing of certain Acts (Trust Services Act)), see §7 (2).

[25] Qualified trust service providers are required to maintain a record of timestamps issued which could be used to find the earliest timestamp of a particular signature (assuming TSP who issued the earliest timestamp is known). See: ETSI EN 319 421 V1.1.1 – Policy and Security Requirements for Trust Service Providers issuing Time-Stamps: https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf, section 7.12.

[26] ETSI standard TS 119 172-4 (Signature validation policy for European qualified electronic signatures/seals using trusted lists) is currently being drafted.

validating digital signatures created under DSA legal requirements. To conclude whether a document bears a valid digital signature, the parties use state-provided signature validation software that contains a validation algorithm implemented as understood by software developers. It would be the task of experts to explain to the court that the current algorithm used by the software does not satisfy the legal requirements.

For most types of contracts, an invalid digital signature will not invalidate the transaction. However, such transactions will not enjoy the presumption of authenticity of digitally signed documents as included in subsection 277(3) of CoCP. This means that burden of proof will shift and it will be on the relying party to prove the intent of parties to enter the particular transaction.

In Estonian law, there are several types of contracts that are valid only in written form. Such contracts include contracts of consumer surety, contracts relating to the purchase of the right to use the building on a timeshare basis, long-term holiday product contracts, exchange system contracts, agency agreements and life annuity contracts. Additionally, as required by law, many applications and declarations of will must follow the written form.

In accordance with the provisions of subsection 80(1) and clause 80(2)(3) of the GPoCCA, a transaction in electronic form is deemed to be equal to a transaction in written form. In order to comply with the requirements for electronic form, a transaction is to be electronically signed by the persons entering into the transaction. The transaction needs to be digitally signed, and the signature must be in conformity with the requirements of law for it to be considered equal to written form.[27]

Substituting paper documents containing handwritten signatures with electronic documents that have been digitally signed is widely practiced in Estonia. The question arises, whether an electronic document, bearing a non-compliant digital signature, can be considered a valid transaction in electronic form within the meaning of Estonian law. To illustrate this, consider a judgment of the Harju County Court in 2016,[28] which dealt with authentication and the digital signature. A customer allegedly authenticated himself through an online bank link to obtain access to the online client system of a chain of petrol stations. The allegation was that the customer ordered a client card and used it to buy petrol. The petrol station chain sent an invoice to the customer's alleged e-mail address. The invoice was not paid. The petrol station chain initiated legal action for the debt. The customer claimed that he had not signed any contract, had not bought any petrol, and the contact information (mobile telephone number and e-mail address) used in the petrol station chain's online client system was not known to him. The court found that authentication via an online bank link is not the equivalent of providing a digital signature. Authentication alone does not prove a transaction was made. The judge found that the petrol station chain had no claim against the customer. The Tallinn Circuit Court upheld the judgement in its 18 January 2017 ruling,[29] and further explained that a digital signature adhering to GPoCCA subsection 80(3) is a prerequisite that needs to be fulfilled to consider a transaction to be made in electronic form.

The decision of the Tallinn Circuit Court established that there can be no valid transaction in electronic form where an electronic document exists without a digital signature, or where the signature itself does not fulfil the requirements set out in GPoCCA subsection 80 (3).

Interestingly, most administrative acts and court judgements in Estonia have also been signed digitally for the last decade. Subsection 441(1) of the CoCP requires judgements to be prepared electronically and to be signed with a digital signature by the judge who made the judgement. The importance of signatures in administrative acts imposing coercive measures was analysed by the Supreme Court in its judgement 3-3-1-71-05 of 22 February 2006.[30] The Administrative Chamber of the Supreme Court explained that the issuing official must sign an administrative act. The requirement of signing is not just a question of form, but the signature proves that the administrative act was issued, and that it was issued by the person signing the act. Decisions to impose coercive measures have legal significance only if they are signed by a competent authority. An unsigned administrative act cannot be considered valid. The Estonian Supreme Court judgement 3-3-1-1-08 of 1

[27] K. Sein. § 80, 3.1. – Tsiviilseadustiku üldosa seadus. Kommenteeritud väljaannne (Commentaries of the General Part of Civil Code Act). Tallinn: Juura 2010.
[28] HMKo 12.10.2016, 2-16-105846.
[29] TlnRnKo 18.01.2017, 2-16-105846.
[30] RKHKo 22.02.2006, 3-3-1-71-05.

November 2007[31] analysed the outcome of a missing signature in a court judgement in administrative proceedings. The Administrative Chamber of the Supreme Court found that the absence of a judge's signature constitutes an absolute ground for annulment. Administrative courts apply the same rules as civil courts. Therefore, the absence of a judge's signature in a civil case judgement would also constitute an absolute ground for annulment.

The validity of a digital signature regarding an arrest in criminal proceedings was considered by Estonian Supreme Court ruling 3-1-1-45-15 of 1 June 2015.[32] The county court judge had digitally signed an arrest warrant, but according to the signature container, his signature was invalid. It was not possible to confirm the validity of the certificate used by the judge at the time of signing. The Criminal Chamber of the Supreme Court found that since only a valid digital signature has legal force, an invalid digital signature must be equated with the absence of a signature and considered a significant violation of criminal procedure. The county court ruling had to be annulled by the district court.

It follows from the cases before the Estonian Supreme Court, that an invalid or missing signature gives a basis for annulment for all court judgements. Furthermore, administrative acts imposing coercive measures carrying an invalid signature cannot be considered valid. An invalid digital signature can have far-reaching consequences, although the question of validity has yet to be tested in court.

Contesting the purported signatory of a digitally signed document

Subsection 277 (3) of the CoCP provides as follows:

> 'Digitaalallkirjaga varustatud elektroonilise dokumendi ehtsust saab vaidlustada üksnes asjaolude põhistamisega, mille põhjal võib eeldada, et dokumenti ei ole koostanud digitaalallkirja omaja.'
>
> 'Authenticity of an electronic document bearing a digital signature may be contested only by substantiating the circumstances which give reason to presume that the document has not been prepared by the holder of the digital signature.'

It is rare for digitally signed electronic documents to be challenged in Estonia. However, when the purported signatory contests the authenticity of a digital signature, the courts have relied on the time of signing to establish the circumstances where the signatory could not have given the signature.

A judgment of the Harju County Court[33] is one of the few examples where a digitally signed electronic contract of suretyship was successfully contested. A lender signed an electronic loan agreement with a borrower and an additional contract of suretyship with a surety without meeting the surety in person. After the borrower failed to repay the loan, the lender filed an action against both. The borrower and surety both gave testimony that the borrower (who, at the time of signing, was a domestic partner to the surety) had stolen his partner's ID card from her purse and found the PIN required for her digital signature in a recipe notebook, which she kept on the kitchen shelf. The judgement was largely based on the testimonies, as well as the fact that the loan agreement and the contract of suretyship were signed in a short two-minute timeframe. This, the court thought, corresponded to the average time it takes to replace the ID card in the reader, wait for the signing application to run and use the PIN. It was determined that both contracts were signed by the lender and borrower. The signature of the surety was added by the borrower, using his partner's ID card and PIN code without her knowledge. Therefore, the county court judge found that the lender had no claim against the surety, since the partner had never signed the contract of suretyship.

An alternative, and more frequent picture, is portrayed in Harju County Court judgement 2-10-30536 of 15 March 2013.[34] A company ran an online auction site brokering loan agreements between investors and clients. A borrower became a member of the online auction site on 31 January 2010 when she digitally signed the auction site's user agreement. On 14 February 2010, she digitally signed 16 electronic loan agreements through the online auction site, received investors' money to her user account and three days later transferred it to her bank account by digitally signing a payment order. She did not log into the auction site after 1 April 2010 and did not repay the loans. The investors assigned their claims to the broker who filed action against the

[31] RKHKo 01.11.2007, 3-3-1-67-07.
[32] RKKKm 01.06.2015, 3-1-1-45-15.
[33] HMKo 10.02.2014, 2-13-34835.
[34] HMKo 15.03.2013, 2-10-30536.

borrower. In court, the borrower claimed that (i) she did not provide the digital signatures, (ii) she did not know how digital signatures worked, and (iii) she had not received any money. She claimed that she gave her ID card and PIN to an acquaintance who abused her trust. However, she could not explain in detail why she would give her ID card away or how the card was used. The county court found that by handing over her ID card to another person, the borrower had to accept undesirable consequences, such as transactions made on her behalf. Since the money was transferred to her bank account, she was also considered to be the recipient of the loans. Therefore, she had to repay the loans and accessory expenses.

As seen in the judgement 2-13-34835, the time of signing might play an important role in establishing the actual signatory. One might criticise the court for basing the judgement on the short time period between the signature and the purported signatory's testimony, and failing to consider the possibility that there was an agreement between former domestic partners that the borrower takes the blame and effectively rescinds the surety's contracts of suretyship.

The uncertainty of time of signing and the ability to effectively change the 'Signed on' time shown by validation software must always be taken into account when considering as evidence the time or time period when electronic documents were signed. This uncertainty gives further possibilities for parties to contest digitally signed documents.[35]

Solutions

Establishing the time of signing in a trusted manner

The obvious solution for the problems described above would be to implement a technical solution that establishes the time of signing in a trusted manner. Such a solution would require the signatories themselves, in the process of creating the digital signature, to interact in an authenticated manner with a trust service provider, which would then attest to the precise time of signing and certificate validity at that time. Currently, for the majority of the digital signatures that are created, it is the party relying on the signature (such as an online bank) who contacts the trust service provider to add a valid timestamp to the signatory's signature.[36] Even if a technical solution were built, it would not be compliant with eIDAS, since eIDAS specifically forbids national law to redefine the eIDAS requirements, where a qualified electronic signature has the equivalent legal effect of a handwritten signature.

Consider case of digital signature solutions such as Mobile-ID.[37] Here, the signatory can only create a digital signature through interaction with the Mobile-ID service provider. In case of doubt, the court can try to establish the time of signing by requesting the respective information[38] from the Mobile-ID service provider.

If the signatory wants to create evidence of a narrow time period when the signature was given, he can use the state-provided signing application, and re-sign the whole digital signature container immediately after it has been signed. The time of signing would then fall in the time period between 'Signed on' time of the inner and outer signature containers. Such a double signature mechanism would also prove that the certificate was valid at the time of signing, assuming evidence can be obtained to prove that the signatory's certificate was not suspended in the relevant time period.

Preventing significant modification of time of signing by non-signatories

The ETSI digital signature format standard suggests a technical solution that could be used to prevent significant modification of time of signing by a non-signatory:

> 'The validation mandated by the signature policy can specify a maximum acceptable time difference which is allowed between the time indicated in the SigningTime element and the time indicated by the SignatureTimeStamp element. If this delay is exceeded, the

[35] For a further discussion about 'non-repudiation' see: S. Mason. Electronic Signatures in Law (4th edition). Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016, 16.14-16.26: open source at https://humanities-digital-library.org/index.php/hdl/catalog/series/observinglaw.

[36] Digitaalset allkirja kasutavate tööealiste (15-64-aastased) Euroopa liidu elanike osakaalu määramine 2015. aastal. Uuringu aruanne. Detsember 2015. https://mkm.ee/sites/default/files/digitaalse_allkirja_kasutamise_osakaalu_uuringu_aruanne_printimiseks.pdf, section 3.2.

[37] See more about Mobile-ID: https://www.id.ee/index.php?id=36882.

[38] The time when signing request was sent to signatory's mobile telephone and the time when signed response was returned.

> electronic signature shall be considered invalid.'[39]

Essentially, it would prevent third parties from obtaining a valid timestamp if the time difference between signatory's self-reported computer time and current time is too large.

However, the problem of establishing the certificate's validity at the time of signing cannot be solved by this mechanism. A malicious party abusing the signatory's signature creation data can set the self-reported computer time to a time in the future, and thus is able to obtain a valid timestamp in the future, after the certificate becomes valid. Furthermore, the use of such an arbitrary 'validation policy' is problematic, since in this case the validity of a digital signature would depend on the permitted time difference specified by the policy and hence would create a legal uncertainty in the validity of the signature, unless the policy is accepted by all the parties involved.

Establishing the validity of a certificate at the time of signing

Since establishing the time of signing in a trusted manner is not a viable solution, we suggest it is necessary to solve the issues that prevent establishing the validity of the certificate at the time of signing. As described above, the timestamping mechanism currently in use could prove the validity of the certificate at the time of signing if it is possible to prevent the status of an invalid certificate to change to being valid. Next, we discuss how to eliminate this problem for cases arising from EITSETA subsection 16(4) and sections 17 and 18.

Certificate validity before QSCD is delivered to the signatory

The solution would be to repeal EITSETA subsection 16(4), thus making the certificate valid from the time of its issuance. Such an amendment on its own, however, would not solve the security risk of a signature being given before the signature creation data in the form of a QSCD is delivered to the signatory. This risk has been highlighted by the recent discovery that the security envelopes holding ID card PINs (signature activation data) were not opaque,[40] allowing the employees of the document issuer to learn the codes and use the ID card before it is delivered to the cardholder. To mitigate this risk, the technical solution should be modified so that the certificate is issued after the QSCD has been delivered to signatory. This has already been implemented for Mobile-ID, where the certificate for Mobile-ID is issued only after the signatory has confirmed that QSCD is in the signatory's possession.[41]

We note that an unauthorised use of QSCD before the certificate is issued does not create a risk – at least in the context of the qualified electronic signature. This is because it is necessary, when creating a valid digital signature in compliance with the eIDAS digital signature format specifications, that the signer's certificate has to be included under the signature and hence must be known at the time of signing.

Issuing a certificate after QSCD is delivered to the signatory will not mitigate the fundamental risk that a qualified trust service provider can create copies of signature creation data and abuse them after QSCD has been delivered to the signatory. However, the risk of third parties abusing QSCD before it is delivered to the signatory is more likely than the risks in the controlled process of generating signature creation data. Therefore, we argue that the law should not hold a signatory liable for signatures made before QSCD has been delivered, unless the risk of abuse of the QSCD before its delivery has been mitigated using effective measures.

Certificate suspension

The legal solution to the certificate suspension problem would be to amend EITSETA subsection 17(5) as follows:

> 'E-signatures or e-seals given during the period when a certificate is suspended are invalid only when the certificate suspension is followed by certificate revocation.'

This text illustrates that the legal definition clearly reflects the technical reality. If the validity of a certificate is suspended and the suspension is never

[39] ETSI TS 101 903 V1.4.2 (2010-12). Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES). Technical Specification: http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf, section 7.3, paragraph 7.

[40] ERR. New ID card issue: Codes can be read using torch, without opening envelope, 20.12.2018. https://news.err.ee/886313/new-id-card-issue-codes-can-be-read-using-torch-without-opening-envelope.

[41] SK ID Solutions AS – Certificate Policy for Mobile ID of the Republic of Estonia. Version 6.0. OID: 1.3.6.1.4.1.10015.1.3. Effective since 24.10.2017: https://sk.ee/upload/files/SK-CP-MOBILE%20ID-EN-v6_0-20171024.pdf, section 4.1.2.

terminated, the signatures made in the period of suspension would not be valid, since a valid timestamp for the signature cannot be obtained. On the other hand, if the suspension is terminated, the signatures made in the period of suspension can be supplemented with a valid timestamp and hence become valid. The termination of suspension would require the signatory to be confident that in the period of suspension the signature creation data was not abused. However, such an amendment to EITSETA subsection 17(5) would be in conflict with eIDAS article 28(5)(a):[42] 'If a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension.' Therefore, the only viable solution is to abandon the option for temporary suspension, leaving certificate revocation the only option. According to the provisions of EITSETA subsection 17(6), trust service providers are not required to support suspension, providing revocation is supported.

The main benefit of the certificate suspension mechanism is that it is possible to restore the validity of the certificate by later terminating the suspension without replacing the QSCD. We note that the same level of convenience can be achieved using the revocation mechanism, assuming a technical solution is used that would allow the signatory to obtain a new certificate without replacing the existing QSCD. The document issuer has already developed such a solution, but until now it has only been used for fixing security flaws and for replacing defective ID card certificates.

Conclusions and recommendations

Contrary to common belief, the technical solution used in the Estonian digital signature scheme does not provide proof of the time when the signature was given. Introducing such a solution would require significant changes to the digital signature scheme, which would not be compatible with eIDAS and the digital signature standards that comply with eIDAS. Therefore, we recommend abandoning the legal requirement to establish the time of signing, which is currently in conflict with eIDAS, by updating the definition of electronic signature as set out in GPoCCA. We also suggest amending EITSETA clause 25(1)(3) to note that the requirement to determine the time of signing does not apply to digital signatures given after 1 July 2016.

Although the eIDAS definition of a qualified electronic signature does not make it necessary to establish the time when the signature was given, the evidentiary value of the digital signature has not changed in practice after eIDAS came into force, because the technical solution used in Estonia has never provided proof of the time of signing. This, however, questions the validity of all Estonian digital signatures created before eIDAS came into force.

Even today, the Estonian public is not aware of the unreliability of the time of signing provided by the digital signature scheme. It follows that a public awareness campaign would be helpful. As a minimum, the description of 'Signed on' time shown in the state-provided validation application should be updated to reflect the technical reality and unreliability of the time shown. The judiciary should also be made aware of these deficiencies. Additionally, we recommend ending the practice of referring to the time of signing for determining any date in a digitally signed document and instead always specify dates of legal significance in the electronic document to be signed.

The validation process of the signature produced by the Estonian digital signature scheme does not and has never provided the assurance that the signatory's certificate was valid at the time of signing. This questions the validity of all digital signatures. To solve this problem for future digital signatures, we recommend that EITSETA be amended to provide that certificates are valid from the beginning of their issuance until expiration or irrevocable revocation. This would also require changes to the lifecycle of QSCD. Namely, making sure that the certificate is issued after QSCD has been delivered to the signatory, and the certificate revocation and renewal process being adjusted to provide the same level of convenience as the current certificate suspension mechanism provides.

We note that the same problem is likely to be present in digital signature schemes used in other EU member states, because the eIDAS technical standards currently do not provide a mechanism which would satisfy the eIDAS legal requirements for signature validation in case the validity of a suspended certificate is restored, or the certificate does not

[42] Despite the conflict with eIDAS, this notion of suspension is followed in Austrian Signatur- und Vertrauensdienstegesetz (Signature and Trust Services Act), see § 6(3) of Section 1 and Croatian Pravilnik o pružanju i korištenju usluga povjerenja (Ordinance on the provision and use of trust services), see article 37(3).

become valid from the moment of its issuance. As a minimum, we recommend updating the eIDAS technical standards to include such warning.

As a temporary technical workaround for signatories wishing to create a digital signature with higher evidentiary value about the time of signing and certificate's validity at the time of signing, we recommend the electronic document should be signed, and then the signatory should immediately sign the whole signature container again. In the long-term, the development of suitable technical standards for solutions that allow the time of signing to be established should be considered, since the ability to establish the time of signing could provide a higher evidentiary value for the digital signature in general, thereby facilitating the use of electronic documents.

Tõnu Mets is a member of the editorial board and a PhD candidate at the School of Law, University of Tartu. His research focuses on the admissibility of digital evidence.

http://mets.law/

Arnis Parsovs is a researcher at STACC OÜ and a PhD candidate at the Computer Science programme, University of Tartu, Estonia. His research focuses on the security of electronic identity, and was supported by the European Regional Development Fund through the Estonian Centre of Excellence in ICT Research under grant number EU48684.